# A RESIDUE SCALAR PRODUCT FOR ALGEBRAIC FUNCTION FIELDS OVER A NUMBER FIELD

XIAN-JIN LI

Abstract. In 1953 Peter Roquette gave an arithmetic proof of the Riemann hypothesis for algebraic function fields over a finite constants field, which was proved by André Weil in 1940. The construction of Weil's scalar product is essential in Roquette's theory. In this paper a scalar product for algebraic function fields over a number field is constructed which is the analogue of Weil's scalar product.

## 1. Introduction

In 1953, Roquette [8] gave an arithmetic proof of the Riemann hypothesis for algebraic function fields over a finite constants field, which was proved by André Weil in 1940 [9]. Since the analogy between number fields and function fields over a finite constants field is rather striking, a question is to generalize Roquette's theory to number fields. Since the analogue of Roquette's theory for number fields does not exist, we want to find the analogue of Roquette's theory for function fields over number fields. The construction of Weil's scalar product is essential in Roquette's theory. In this paper a scalar product for function fields over number fields is constructed which is the analogue of Weil's scalar product.

This paper is organized as follows: In Section 2, a set of prime divisors is given on which we base our constructions. In Section 3, we establish some properties about the set of multiples of a divisor (cf. [5, Chapter 24]). These properties are essential for our definition of divisor residues. Divisor residues are then defined in Section 4, and they are closely related to the theory of correspondences. Divisor residues may not lie in the given function fields. In Section 5, we use the norm to obtain divisors of the given function field from divisor residues. Next in Section 6, we consider function fields over complex numbers which have the structure of compact Riemann surfaces. In this section we make use of the Arakelov theory to complete our definition of a residue scalar product for algebraic function fields over a number field.

Assume that $k$ is a number field. By the field of algebraic functions of one variable over $k$ we mean a field, which contains a transcendental element $x$ and is a finite algebraic extension of the rational function field $k(x)$. Let $K$ and $K'$ be two function fields of one variable which are finite extensions of $k(x)$ and $k(x')$, respectively, with $x$ and $x'$ being two algebraically independent elements over $k$. The

1991 *Mathematics Subject Classification.* Primary 11R58, 12E30.

*Key words and phrases.* Function fields, Riemann hypotheses.

Research supported by the American Institute of Mathematics.

double field $\Delta$ of $K$ and $K'$ is defined to be the field $k(x,x';u,u')$ with $f(x,u)=0$ and $f'(x',u')=0$ over $k$, where $f$ and $f'$ are generating irreducible polynomials of $K$ and $K'$ over $k$, respectively. Valuations of $k(x,x')$, which are derived from irreducible polynomials of $k[x,x']$, from the negative degree of $x$, and from the negative degree of $x'$, correspond to prime divisors of the rational function field $k(x,x')$. Our construction of a residue scalar product is based on those prime divisors of $\Delta$ lying over the above prime divisors of $k(x,x')$. A characterization for these prime divisors of the double field $\Delta$ is given in Theorem 2.1.

To proceed our construction, we start with the multiple ideal of a divisor, which is a extremely useful tool for this paper. Let $\mathfrak{o}$ be a prime divisor of $K$, and let $\mathfrak{o}'$ be a prime divisor of $K'$. If $\mathfrak{A}$ is a divisor of the double field $\Delta$, the multiple ideal $[\mathfrak{A}]_{(\mathfrak{o},\mathfrak{o}')}$ is the set of all elements $a$ of $\Delta$ such that $w_{\mathfrak{o}}(a)\geqslant w_{\mathfrak{o}}(\mathfrak{A})$, $w_{\mathfrak{o}'}(a)\geqslant w_{\mathfrak{o}'}(\mathfrak{A})$, and $w_{\mathfrak{m}}(a)\geqslant w_{\mathfrak{m}}(\mathfrak{A})$ for all prime divisors $\mathfrak{m}$ of $\Delta$ lying over those prime divisors of $k(x,x')$ which correspond to two variable irreducible polynomials of $k[x,x']$. Assume that $\tilde{K}'$ is a finite extension of $K'$. Let $\tilde{\mathfrak{A}}$ be the extension of $\mathfrak{A}$ in the double field of $K,\tilde{K}'$, and let $\tilde{\mathfrak{o}}'$ be a prime divisor of $\tilde{K}'$ lying over $\mathfrak{o}'$. A relation between the multiple ideals $[\mathfrak{A}]_{(\mathfrak{o},\mathfrak{o}')}$ and $[\tilde{\mathfrak{A}}]_{(\mathfrak{o},\tilde{\mathfrak{o}}')}$ is obtained in Theorem 3.3, which will be used in later proofs.

Let $\mathfrak{n}$ be a prime divisor of the double field $\Delta$, and let $\mathfrak{A}$ be a divisor of $\Delta$, prime to $\mathfrak{n}$. If $\bar{\mathfrak{o}}$ be a prime divisor of the residue field $\Delta\mathfrak{n}$ of $\Delta$ modulo $\mathfrak{n}$, we denote $w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n})=\min_{a\in[\mathfrak{A}]_{\underline{\mu}\bar{\mathfrak{o}}}} w_{\bar{\mathfrak{o}}}(a\mathfrak{n})$, where $\underline{\mu}\bar{\mathfrak{o}}$ is a pair of prime divisors of $K,K'$ obtained from $\bar{\mathfrak{o}}$. A precise formula for $\underline{\mu}\bar{\mathfrak{o}}$ is given in Section 4. Then the divisor residue of $\mathfrak{A}$ modulo $\mathfrak{n}$ is defined by

$$\mathfrak{A}\mathfrak{n}=\sum w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n})\bar{\mathfrak{o}}$$

where the sum is over all prime divisors $\bar{\mathfrak{o}}$ of $\Delta\mathfrak{n}$. It is easy to see that if $\mathfrak{A}$ is principal, so is $\mathfrak{A}\mathfrak{n}$. If $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are two divisors of $\Delta$, prime to $\mathfrak{n}$, we prove in Theorem 4.8 that $(\mathfrak{A}_1+\mathfrak{A}_2)\mathfrak{n}=\mathfrak{A}_1\mathfrak{n}+\mathfrak{A}_2\mathfrak{n}$. The divisor residues are closely related to the theory of correspondence, and a relation between them is given in Theorem 4.11.

Let $\mathfrak{A}$ and $\mathfrak{b}$ be divisors of $\Delta$, relatively prime to each other. Write $\mathfrak{A}=\sum a_{\mathfrak{m}}\mathfrak{m}$ and $\mathfrak{b}=\sum b_{\mathfrak{n}}\mathfrak{n}$ as linear combination of prime divisors of $\Delta$ with integer coefficients. Define

$$\langle\mathfrak{A},\mathfrak{b}\rangle_{f'}=\sum_{\mathfrak{m},\mathfrak{n}} a_{\mathfrak{m}}b_{\mathfrak{n}}\mathfrak{N}_{\Delta\mathfrak{n}/K'\nu'}(\mathfrak{m}\mathfrak{n}){\nu'}^{-1}$$

where $\mathfrak{N}_{L/F}$ is the usual notation of norm and $\nu'$ is the isomorphism of $K'$ induced by $\mathfrak{n}$. Then $\langle\mathfrak{A},\mathfrak{b}\rangle_{f'}$ is a divisor of $K'$. By using Theorem 4.8 and Theorem 4.11, we prove in Theorem 5.3 that $\langle\mathfrak{A},\mathfrak{b}\rangle_{f'}=\langle\mathfrak{b},\mathfrak{A}\rangle_{f'}$.

When $K'$ is considered as an algebraic function field of one variable over complex numbers, the set of all places of $K'$ has the structure of a compact Riemann surface which is denoted by $K'_\infty$. If $\mathfrak{A}$ and $\mathfrak{b}$ are divisors of $\Delta$, we can obtain an Arakelov divisor $\langle\mathfrak{A},\mathfrak{b}\rangle_{K'}$ from the divisor $\langle\mathfrak{A},\mathfrak{b}\rangle_{f'}$ by using the extension of $\langle\mathfrak{A},\mathfrak{b}\rangle_{f'}$ to $K'_\infty$; see Section 6. Let $\mathfrak{d}_{K'}$ be a canonical Arakelov divisor of $K'$. Define

$$\langle\mathfrak{A},\mathfrak{b}\rangle=(\langle\mathfrak{A},\mathfrak{b}\rangle_{K'}\cdot\mathfrak{d}_{K'})$$

where $(\,\cdot\,)$ is the Arakelov intersection product. Let $\mathfrak{A}|K'$ be the Arakelov divisor of $K'$ obtained from the restriction of $\mathfrak{A}$ to $K'$. If $\mathfrak{m}$ and $\mathfrak{n}$ are prime divisors of $\Delta$, we define

$$\{\mathfrak{m},\mathfrak{n}\} = N_{\Delta/K'}(\mathfrak{n})\,(\mathfrak{m}|K'\cdot\mathfrak{d}_{K'}) + N_{\Delta/K'}(\mathfrak{m})\,(\mathfrak{n}|K'\cdot\mathfrak{d}_{K'})$$

where $N_{\Delta/K'}(\mathfrak{n}) = [\Delta\mathfrak{n} : K'\nu']$. For general divisors $\mathfrak{A},\mathfrak{b}$ of $\Delta$, we define $\{\mathfrak{A},\mathfrak{b}\}$ by linearity. Then a residue scalar product of $\mathfrak{A},\mathfrak{b}$ is defined by

$$\langle\mathfrak{A},\mathfrak{b}\rangle_r = \{\mathfrak{A},\mathfrak{b}\} - \langle\mathfrak{A},\mathfrak{b}\rangle$$

for all divisors $\mathfrak{A},\mathfrak{b}$ of $\Delta$. By using results of Section 2–5, we proved in Section 6 that the residue scalar product is bilinear and symmetric. It is well-defined on the classes of divisors of $\Delta$ modulo principal divisors.

The author wishes to thank Brian Conrey for his encouragement during preparation of the manuscript.

## 2. Prime divisors

Let $\mu$, $\mu'$ be a pair of isomorphisms of $K$, $K'$ into an algebraic function field $\tilde{K}$ of one variable. Then a dependent composite $M$ of $K$, $K'$ is defined to be the field composite $K\mu\cdot K'\mu'$ in $\tilde{K}$. Consider $M$ as a finite extension of $K'\mu'$. Then there exists an isomorphism $\sigma_0$ of $M$, whose restriction to $K'\mu'$ is ${\mu'}^{-1}$. Denote $\mu_0 = \mu\sigma_0$. Then the representative $M_0 = K\mu_0\cdot K'$ of the dependent composite $M$ is called $K'$-normalized. If $\sigma$ is an isomorphism of $M_0$ over $K'$, then $\mu_0\sigma$ is called a $K'$-conjugate of $\mu_0$. Denote by $\underline{\mu} = \mu_0\underline{\sigma}$ the set of all $K'$-conjugates of $\mu_0$, and $\underline{\mu}$ is called the isomorphism system coordinated to the isomorphism $\mu_0$ of $K$.

If one of the two isomorphisms $\mu$, $\mu'$, say $\mu$, degenerates to a homomorphism, then a prime ideal $\mathfrak{m}$ of $K$ exists such that $\mu$ is the residue class homomorphism modulo $\mathfrak{m}$ of $K$. That is, $a\mu$ is the residue $a\mathfrak{m}$ of $a$ modulo $\mathfrak{m}$ for every element $a$ of $K$, where $a\mathfrak{m}$ represents the symbol $\infty$ when $a$ is not integral for $\mathfrak{m}$. The residue field of $K$ modulo $\mathfrak{m}$ is a finite extension of $k$, and the $K'$-normalized representative of the dependent composite $M$ of $K\mu$, $K'\mu'$ is then a finite constants extension of $K'$.

A binary prime divisor $\mathfrak{m}$ of $\Delta$ is defined to be a non-equivalent normalized valuation $w_{\mathfrak{m}}$ of $\Delta$ which valuates both $K$ and $K'$ identically zero, a $K$-unary prime divisor $\mathfrak{m}$ of $\Delta$ is a non-equivalent normalized valuation $w_{\mathfrak{m}}$ of $\Delta$ which valuates $K'$ identically zero, and a prime $K'$-unary divisor $\mathfrak{m}$ of $\Delta$ is a non-equivalent normalized valuation $w_{\mathfrak{m}}$ of $\Delta$ which valuates $K$ identically zero. Denote by $S$ the set of all binary and unary prime divisors of $\Delta$.

In particular, binary prime divisors of the rational function field $k(x,x')$ correspond to valuations derived from irreducible "binary" polynomials of $k[x,x']$, $k(x)$-unary prime divisors of $k(x,x')$ correspond to valuations derived from irreducible polynomials of $k[x]$ and to the valuation given by the negative degree in $x$, and $k(x')$-unary prime divisors of $k(x,x')$ correspond to valuations derived from irreducible polynomials of $k[x']$ and to the valuation given by the negative degree in

$x'$. Since $\Delta$ is a finite separable extension of $k(x, x')$, all prime divisors of $\Delta$ in $S$ are obtained from the corresponding three kinds of prime divisors of $k(x, x')$ by extension of valuations under finite separable extension of fields (cf. [3, §10]). The following Lemma gives a characterization of prime divisors of $\Delta$ in $S$.

**Theorem 2.1.** *The prime divisors $\mathfrak{m}$ of $\Delta$ in $S$ are in one-one correspondence with the classes of isomorphism pairs $\mu$, $\mu'$ of $K$, $K'$ into an algebraic function field of one variable in such a way that the residue class homomorphism of $\Delta$ modulo $\mathfrak{m}$ induces the isomorphism pair $\mu$, $\mu'$ and that*

$$\Delta\mathfrak{m} = K\mu \cdot K'\mu'.$$

*Proof.* Let $\mathfrak{m}$ be a prime divisor of $\Delta$. Then the residue class homomorphism of $\Delta$ modulo $\mathfrak{m}$ induces isomorphisms or homomorphisms $\mu$, $\mu'$ of $K$, $K'$ into the residue class field $\Delta\mathfrak{m}$, which is an algebraic function field of one variable. It is clear that $\Delta\mathfrak{m} = K\mu \cdot K'\mu'$, and hence, $\mathfrak{m}$ induces the class of isomorphism pair $\mu$, $\mu'$ of $K$, $K'$ satisfying $\Delta\mathfrak{m} = K\mu \cdot K'\mu'$.

Conversely, let $\mu$, $\mu'$ be an isomorphism pair of $K$, $K'$ into an algebraic function field, which do not both degenerate to homomorphisms. Assume that $\mu'$ does not degenerate to a homomorphism. Then the $K'$-normalized representative of the dependent composite $K\mu \cdot K'\mu'$ is of the form $K\mu_0 \cdot K'$. A prime divisor $\mathfrak{m}$ of $\Delta$ exists such that $\Delta\mathfrak{m} = K\mu_0 \cdot K'$. It follows that the residue homomorphism of $\Delta$ modulo $\mathfrak{m}$ induces the isomorphism pair $\mu_0$, 1 of $K$, $K'$, and $\mathfrak{m}$ is uniquely determined by the class of $K'$-conjugates of $\mu_0$. Therefore, a unique prime divisor $\mathfrak{m}$ of $\Delta$ exists, which corresponds to the class of isomorphism pair $\mu$, $\mu'$ of $K$, $K'$ in such a way that the residue class homomorphism of $\Delta$ modulo $\mathfrak{m}$ induces $\mu$, $\mu'$ and $\Delta\mathfrak{m} = K\mu \cdot K'\mu'$.

This completes the proof of the theorem.

**Corollary 2.2.** *The $K$-unary and $K'$-unary prime divisors of $\Delta$ are in one-one correspondence with the prime divisors of $K$ and $K'$, respectively.*

Divisors $\mathfrak{A}$ of $\Delta$ are defined as the formal sum

$$\mathfrak{A} = \sum w_{\mathfrak{m}}(\mathfrak{A})\mathfrak{m}$$

where the sum is over all prime divisors $\mathfrak{m}$ in $S$ with the integer coefficients $w_{\mathfrak{m}}(\mathfrak{A})$ being zero for almost all prime divisors $\mathfrak{m}$.

## 3. The ideal of multiples of a divisor

In this section, we study some properties of multiple ideals, which are essential for our definition of divisor residues given in the next section.

Let $J$ be the set of all elements in $\Delta$ which are integral for all binary prime divisors of $\Delta$. Let $\mathfrak{o}$ and $\mathfrak{o}'$ be $K$-unary and $K'$-unary prime divisors of $\Delta$, respectively. Denote $\underline{\mathfrak{o}} = (\mathfrak{o}, \mathfrak{o}')$. The principal order $J_{\underline{\mathfrak{o}}}$, restricted by the unary pair $\underline{\mathfrak{o}}$, is the set of all elements of $\Delta$ which are integral for all binary prime divisors and for the unary pair.

**Lemma 3.1.** *$J$ is the ring composite $[K, K']$ of $K$ and $K'$.*

*Proof.* It is clear that $[K, K']$ is contained in $J$. Conversely, let $a$ be a nonzero element of $J$. Then the denominator $n$ of $a$ contains only unary prime divisors. Let $t$ be a non-constant element of $K$ whose denominator contains all prime divisors of $K$ dividing $n$. Since $K$ is a finite algebraic extension of $k(t)$, we can choose a $t$-integral basis $u_i$ of $K$ over the field $k(t)$. Then the $u_i$ also form a basis of $\Delta$ over $K'(t)$. Since $a$ is integral in $t$, it can be written in the form $a = \sum f'_i(t)u_i$ with $f'_i(t)$ in $K'[t]$. It follows that $a$ belongs to the ring composite $[K, K']$. $\square$

Let $\mathfrak{A}$ be a divisor of $\Delta$. The $J$-multiple ideal $[\mathfrak{A}]$ of $\mathfrak{A}$ is the set of all elements $a$ in $\Delta$ such that $w_{\mathfrak{m}}(a) \geq w_{\mathfrak{m}}(\mathfrak{A})$ for all binary prime divisors $\mathfrak{m}$ of $\Delta$. Let $\tilde{K'}$ be a finite extension of $K'$. Put $\tilde{J} = [K, \tilde{K'}]$. Let $\tilde{\mathfrak{A}}$ be the extension of a divisor $\mathfrak{A}$ of $\Delta$ in the double field $\tilde{\Delta}$ of $K$ and $\tilde{K'}$. Then the $\tilde{J}$-multiple ideal $[\tilde{\mathfrak{A}}]$ of $\tilde{\mathfrak{A}}$ in $\tilde{\Delta}$ is $[\mathfrak{A}]\tilde{J}$. In fact, since the extension $\tilde{\Delta}$ of $\Delta$ can be considered as the extension $\tilde{K'}$ of $K'$ over $K$, every binary prime divisor of $\Delta$ splits into binary prime divisors of $\tilde{\Delta}$. Since binary prime divisors of $\Delta$ form a proper subset of prime divisors of $\Delta/K$, considered as an algebraic function field of one variable over $K$, by strong approximation theorem (cf. [5, Chapter 24]) we find that $\tilde{\mathfrak{A}}$ is the greatest common binary divisor of all elements in the $\tilde{J}$-ideal $[\mathfrak{A}]\tilde{J}$. Since binary prime divisors of $\tilde{\Delta}$ form a proper subset of prime divisors of $\tilde{\Delta}/K$, by strong approximation theorem we also find that $\tilde{\mathfrak{A}}$ is the greatest common binary divisor of all elements in the $\tilde{J}$-ideal $[\tilde{\mathfrak{A}}]$. Therefore, we have $[\mathfrak{A}]\tilde{J} = [\tilde{\mathfrak{A}}]$.

Let $\mathfrak{o}$, $\mathfrak{o}'$ be prime divisors of $K$, $K'$, and let $1_{\mathfrak{o}}$, $1'_{\mathfrak{o}'}$ be the sets of all elements in $K$, $K'$ which are integral for $\mathfrak{o}$, $\mathfrak{o}'$, respectively.

**Lemma 3.2.** $J_{\underline{\mathfrak{o}}} = [1_{\mathfrak{o}}, 1'_{\mathfrak{o}'}]$.

*Proof.* It is clear that $[1_{\mathfrak{o}}, 1'_{\mathfrak{o}'}]$ is contained in $J_{\underline{\mathfrak{o}}}$. Conversely, let $a$ be an element in $J_{\underline{\mathfrak{o}}}$. Then the denominator $n$ of $a$ contains only unary prime divisors of $\Delta$ different from $\mathfrak{o}$, $\mathfrak{o}'$. Let $t$ be a non-constant $\mathfrak{o}$-integral element in $K$ whose denominator contains all prime divisors of $K$ dividing $n$. Choose a $t$-integral basis $u_i$ for $K$ over $k(t)$. Then the $u_i$ are $\mathfrak{o}$-integral. Write

$$a = \sum_i \sum_{k \geq 0} a'_{ik} t^k u_i$$

with $a'_{ik}$ in $K'$. This implies that $a$ belongs to $[1_{\mathfrak{o}}, K']$.

Since $t^k u_i$ is in $K$, we have $w_{\mathfrak{o}'}(t^k u_i) = 0$. Hence, $w_{\mathfrak{o}'}(a) \geq \min_{i,k} w_{\mathfrak{o}'}(a'_{ik}) = \ell$. We want to show that $\ell$ is nonnegative. Arguing by contradiction, assume that $\ell$ is a negative integer. Let $\pi'$ be a prime element of $\mathfrak{o}'$ in $K'$. Define $b'_{ik} = {\pi'}^{-\ell} a'_{ik}$. Since $a$ is integral for $\mathfrak{o}'$, we have

$$\sum_i \sum_{k \geq 0} b'_{ik} t^k u_i \equiv 0 \mod \mathfrak{o}'.$$

Replacing the $b'_{ik}$ by its residues modulo $\mathfrak{o}'$, we obtain an equation of the $t^k u_i$ with coefficients in the residue class field of $K'$ modulo $\mathfrak{o}'$. Since the $t^k u_i$ are linearly

independent over $k$, by the argument in [2, Chapter 15] they are linearly independent over the residue class field of $K'$ modulo $\mathfrak{o}'$. It follows that these coefficients must be all equal to zero. This is impossible. Therefore, $\ell \geq 0$, and hence $a$ belongs to $[1_{\mathfrak{o}}, 1'_{\mathfrak{o}'}]$. $\square$

Let $\mathfrak{A}$ be a divisor of $\Delta$ and $\underline{\mathfrak{o}} = (\mathfrak{o}, \mathfrak{o}')$ a unary pair. The $J_{\underline{\mathfrak{o}}}$-multiple ideal $[\mathfrak{A}]_{\underline{\mathfrak{o}}}$ of $\mathfrak{A}$ is defined to be the set of all elements $a$ in $\Delta$ such that $w_{\mathfrak{m}}(a) \geq w_{\mathfrak{m}}(\mathfrak{A})$ for all binary prime divisors $\mathfrak{m}$ of $\Delta$ and such that $w_{\mathfrak{o}}(a) \geq w_{\mathfrak{o}}(\mathfrak{A})$, $w_{\mathfrak{o}'}(a) \geq w_{\mathfrak{o}'}(\mathfrak{A})$. Let $\tilde{K}'$ be a finite extension of $K'$. Assume that $\tilde{\mathfrak{o}}'$ is a prime divisor of $\tilde{K}'$ lying above $\mathfrak{o}'$. Denote $\underline{\tilde{\mathfrak{o}}} = (\mathfrak{o}, \tilde{\mathfrak{o}}')$. Define $\tilde{1}'_{\tilde{\mathfrak{o}}'}$ to be the set of all $\tilde{\mathfrak{o}}'$-integral elements of $\tilde{K}'$. Then $\tilde{J}_{\underline{\tilde{\mathfrak{o}}}} = [1_{\mathfrak{o}}, \tilde{1}'_{\tilde{\mathfrak{o}}'}]$.

**Theorem 3.3.** *Let $\mathfrak{A}$ be a divisor of $\Delta$. Then the $\tilde{J}_{\underline{\tilde{\mathfrak{o}}}}$-multiple ideal $[\tilde{\mathfrak{A}}]_{\underline{\tilde{\mathfrak{o}}}}$ of $\tilde{\mathfrak{A}}$ in $\tilde{\Delta}$ is $[\mathfrak{A}]_{\underline{\mathfrak{o}}}\tilde{J}_{\underline{\tilde{\mathfrak{o}}}}$.*

*Proof.* Multiplying $\mathfrak{A}$ by an element of $\Delta$, we can assume that $\mathfrak{A}$ is integral for all binary prime divisors of $\Delta$. It will first be shown that

$$[\tilde{\mathfrak{A}}]_{\underline{\mathfrak{o}}} = [\mathfrak{A}]_{\underline{\mathfrak{o}}}\tilde{J}_{\underline{\mathfrak{o}}},$$

where an element $\tilde{a}$ of $\tilde{\Delta}$ is said be integral for $\mathfrak{o}'$ if $\tilde{a} \equiv 0$ modulo $\mathfrak{o}'$. Let $[\tilde{\mathfrak{A}}]^0_{\underline{\mathfrak{o}}}$ be the set of all $\underline{\mathfrak{o}}$-multiples of $\tilde{\mathfrak{A}}$ in $\tilde{J}_{\underline{\mathfrak{o}}}$. Then $[\tilde{\mathfrak{A}}]_{\underline{\mathfrak{o}}} = [\tilde{\mathfrak{A}}] \cap [\tilde{\mathfrak{A}}]^0_{\underline{\mathfrak{o}}}$. Similarly, we have $[\mathfrak{A}]_{\underline{\mathfrak{o}}} = [\mathfrak{A}] \cap [\mathfrak{A}]^0_{\underline{\mathfrak{o}}}$. Let $\{\tilde{u}'_i\}$ be an $\mathfrak{o}'$-integral basis for $\tilde{K}'$ over $K'$. Then $\tilde{K}' = \sum K'\tilde{u}'_i$ and $\tilde{1}'_{\mathfrak{o}'} = \sum 1'_{\mathfrak{o}'}\tilde{u}'_i$. It follows that $\tilde{J} = [K, \tilde{K}'] = \sum J\tilde{u}'_i$ and $\tilde{J}_{\underline{\mathfrak{o}}} = [1_{\mathfrak{o}}, \tilde{1}'_{\mathfrak{o}'}] = \sum J_{\underline{\mathfrak{o}}}\tilde{u}'_i$. This implies that $[\tilde{\mathfrak{A}}] = [\mathfrak{A}]\tilde{J} = \sum [\mathfrak{A}]\tilde{u}'_i$. Let $a$, $a'$ be elements of $K$, $K'$ such that $w_{\mathfrak{o}}(a) = w_{\mathfrak{o}}(\mathfrak{A})$ and $w_{\mathfrak{o}'}(a') = w_{\mathfrak{o}'}(\mathfrak{A})$. Then $[\tilde{\mathfrak{A}}]^0_{\underline{\mathfrak{o}}} = aa'\tilde{J}_{\underline{\mathfrak{o}}} = \sum aa'J_{\underline{\mathfrak{o}}}\tilde{u}'_i = \sum [\mathfrak{A}]^0_{\underline{\mathfrak{o}}}\tilde{u}'_i$. It follows that $[\tilde{\mathfrak{A}}]_{\underline{\mathfrak{o}}} = [\tilde{\mathfrak{A}}] \cap [\tilde{\mathfrak{A}}]^0_{\underline{\mathfrak{o}}} = \sum([\mathfrak{A}] \cap [\mathfrak{A}]^0_{\underline{\mathfrak{o}}})\tilde{u}'_i = \sum [\mathfrak{A}]_{\underline{\mathfrak{o}}}\tilde{u}'_i = [\mathfrak{A}]_{\underline{\mathfrak{o}}}\tilde{J}_{\underline{\mathfrak{o}}}$. Therefore, in order to prove the stated result it suffices to show that $[\tilde{\mathfrak{A}}]_{\underline{\tilde{\mathfrak{o}}}} = [\tilde{\mathfrak{A}}]_{\underline{\mathfrak{o}}}\tilde{1}'_{\tilde{\mathfrak{o}}'}$. It is clear that $[\tilde{\mathfrak{A}}]_{\underline{\mathfrak{o}}}\tilde{1}'_{\tilde{\mathfrak{o}}'}$ is contained in $[\tilde{\mathfrak{A}}]_{\underline{\tilde{\mathfrak{o}}}}$. Conversely, let $\tilde{a}$ be an element of $\tilde{\Delta}$ in $[\tilde{\mathfrak{A}}]_{\underline{\tilde{\mathfrak{o}}}}$. By strong approximation theorem, we can choose an element $\tilde{n'}$ in $\tilde{K}'$ such that $w_{\tilde{\mathfrak{o}}'}(\tilde{n'}) = 0$ and $w_{\tilde{\mathfrak{o}}'_i}(\tilde{n'}) \geq w_{\tilde{\mathfrak{o}}'_i}(\mathfrak{A}) - w_{\tilde{\mathfrak{o}}'_i}(\tilde{a})$ for every prime divisor $\tilde{\mathfrak{o}}'_i \neq \tilde{\mathfrak{o}}'$ of $\tilde{K}'$ lying above $\mathfrak{o}'$. Then $a\tilde{n'}$ belongs to $[\tilde{\mathfrak{A}}]_{\underline{\mathfrak{o}}}$, and $\tilde{n'}^{-1}$ belongs to $\tilde{1}'_{\tilde{\mathfrak{o}}'}$. Therefore, $\tilde{a}$ belongs to $[\tilde{\mathfrak{A}}]_{\underline{\mathfrak{o}}}\tilde{1}'_{\tilde{\mathfrak{o}}'}$.

This completes the proof of the theorem.

Let $\mathfrak{m}$ be a prime divisor of $\Delta$ with $\mu$, $\mu'$ being the isomorphism pair of $K$, $K'$ induced by $\mathfrak{m}$. If $\mathfrak{m}$ is not $K'$-unary, then degree of $\mathfrak{m}$ over $K'$ is defined by $N_{\Delta/K'}(\mathfrak{m}) = [\Delta\mathfrak{m} : K'\mu']$. And if $\mathfrak{m}$ is not $K$-unary, then the degree of $\mathfrak{m}$ over $K$ is defined by $N_{\Delta/K}(\mathfrak{m}) = [\Delta\mathfrak{m} : K\mu]$. Define $N_{\Delta/K'}(\mathfrak{m}) = 0$ if $\mathfrak{m}$ is $K'$-unary, and define $N_{\Delta/K}(\mathfrak{m}) = 0$ if $\mathfrak{m}$ is $K$-unary. By a splitting field for a binary prime divisor $\mathfrak{m}$ we mean a finite extension $\tilde{K}'$ of $K'$ such that, in the double field $\tilde{\Delta}$ of $K$ and $\tilde{K}'$, $\mathfrak{m}$ splits into prime divisors $\tilde{\mathfrak{m}}$ of degree one over $\tilde{K}'$.

Let $\mathfrak{m}$ be a binary prime divisor of $\Delta$. Assume that the residue class field $\Delta\mathfrak{m}$ is $K'$-normalized and that $\underline{\mu} = \mu\underline{\sigma}$ is the coordinated isomorphism system. Let $\tilde{K}'$ be

a finite extension of $K'$. Decompose $\mu\underline{\sigma}$ into $\tilde{K}'$-conjugate classes with the $\sigma_i$ being representatives for these classes. By Theorem 2.1, let $\tilde{\mathfrak{m}}_i$ be the prime divisor of $\tilde{\Delta}$ corresponding to the $\tilde{K}'$-conjugate class represented by $\mu\sigma_i$. Then the degree of $\tilde{\mathfrak{m}}_i$ over $\tilde{K}'$ is $N_{\tilde{\Delta}/\tilde{K}'}(\tilde{\mathfrak{m}}_i) = [K\mu\sigma_i \cdot \tilde{K}' : \tilde{K}']$. It follows that a finite extension $\tilde{K}'$ of $K'$ is a splitting field of $\mathfrak{m}$ if and only if $K\mu\sigma$ is contained in $\tilde{K}'$ for every isomorphism $\sigma$ of $\Delta\mathfrak{m}$, and that the number of such different prime divisors $\tilde{\mathfrak{m}}_i$ of $\tilde{\Delta}$ lying above $\mathfrak{m}$ is equal to the field extension degree of $\Delta\mathfrak{m}$ over $K'$.

**Lemma 3.4.** *Let $\tilde{K}'$ be a splitting field for a binary prime divisor $\mathfrak{m}$ of $\Delta$. Then $\mathfrak{m}$ is unramified in the double field $\tilde{\Delta}$ of $K$ and $\tilde{K}'$.*

*Proof.* Let $\underline{u'} = \{\tilde{u}'_i\}$ be a basis of $\tilde{K}'$ over $K'$. Then $\underline{u'}$ is also a $\mathfrak{m}$-integral basis for $\tilde{\Delta}$ over $\Delta$. In fact, let $\tilde{a}$ be an $\mathfrak{m}$-integral element in $\tilde{\Delta}$. Multiply $\tilde{a}$ by an element $\tilde{v}$ of $\tilde{\Delta}$, which is prime to $\mathfrak{m}$, so that $\tilde{a}\tilde{v}$ is integral for every binary prime divisor of $\tilde{\Delta}$. Then $\tilde{a}\tilde{v}$ belongs to $\tilde{J}$. Since $\tilde{J} = [K, \tilde{K}'] = \sum J\tilde{u}'_i$, $\tilde{a}$ belongs to $\sum \tilde{v}^{-1}J\tilde{u}'_i$, and hence $\tilde{a}$ can be expressed as a linear combination of $\tilde{u}'_i$ with $\mathfrak{m}$-integral coefficients. Since $\tilde{K}'$ is a splitting field of $\mathfrak{m}$, there exists no $\mathfrak{m}$-integral elements $a_i$ of $\Delta$ such that $\sum a_i\tilde{u}'_i = 0$. Therefore, $\underline{u'}$ is a $\mathfrak{m}$-integral basis for $\tilde{\Delta}$ over $\Delta$.

Since $\tilde{K}'$ is separable over $K'$ and since $\underline{u'}$ is a basis for $\tilde{K}'$ over $K'$, the discriminant $d_{\tilde{K}'/K'}(\underline{u'})$ does not vanish. Since $d_{\tilde{K}'/K'}(\underline{u'})$ is an element of $K'$, $\mathfrak{m}$ is not a divisor of it. Now, the discriminant $d_{\tilde{\Delta}/\Delta}(\underline{u'})$ divides $d_{\tilde{K}'/K'}(\underline{u'})$, and hence $\mathfrak{m}$ is not a divisor of $d_{\tilde{\Delta}/\Delta}(\underline{u'})$. On the other hand, the contribution of $\mathfrak{m}$ to field discriminant $d_{\tilde{\Delta}/\Delta}$ of $\tilde{\Delta}$ over $\Delta$ divides $d_{\tilde{\Delta}/\Delta}(\underline{u'})$. Therefore, $\mathfrak{m}$ is not a divisor of $d_{\tilde{\Delta}/\Delta}$. This implies that $\mathfrak{m}$ is unramified in $\tilde{\Delta}$ by the Dedekind discriminant theorem. □

The following result, which follows immediately from Lemma 3.4 and from the argument preceding Lemma 3.4, is a convenient technique which will be used in later proofs.

**Corollary 3.5.** *Let $\mathfrak{m}$ be a binary prime divisor with $N_{\Delta/K'}(\mathfrak{m}) = n$, and let $\tilde{K}'$ be a splitting field for $\mathfrak{m}$. Assume that the residue class field $\Delta\mathfrak{m}$ is $K'$-normalized and that $\mu\underline{\sigma}$ is the coordinated isomorphism system of $K$ into $\tilde{K}'$. Then $\mathfrak{m}$ has in $\tilde{\Delta}$ the decomposition*

$$\mathfrak{m} = \sum \tilde{\mathfrak{m}}_\sigma$$

*into $n$ prime divisors $\tilde{\mathfrak{m}}_\sigma$ with $N_{\tilde{\Delta}/\tilde{K}'}(\tilde{\mathfrak{m}}_\sigma) = 1$ and with the coordinated isomorphism $\mu\sigma$ of $K$ into $\tilde{K}'$.*

## 4. Definition of divisor residues

We first introduce a notation. If a field $L$ is a finite separable extension of a field $F$, and if $\mathfrak{m}$ is a prime divisor of $F$ whose extension in $L$ has a factorization of the form $\mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_r^{e_r}$, then we define

$$\Pi_{L/F}(\mathfrak{P}_i) = \mathfrak{m}$$

for $i = 1, \cdots, r$, and extend it to the group of all divisors of $L$ by additivity. In other words, $\Pi_{L/F}(\mathfrak{P})$ is a prime divisor of $F$ lying below the prime divisor $\mathfrak{P}$ of $L$.

Let $\mathfrak{n}$ be a prime divisor of $\Delta$ in $S$. Assume that $\underline{\mu} = (\mu, \mu')$ is the isomorphism pair of $K$, $K'$ induced by $\mathfrak{n}$ as in Theorem 2.1. For every prime divisor $\bar{\mathfrak{o}}$ of $\Delta\mathfrak{n}$, define

$$\mu\bar{\mathfrak{o}} = \begin{cases} \mathfrak{n}, & \text{if } \mathfrak{n} \text{ is } K\text{-unary;} \\ \Pi_{\Delta\mathfrak{n}/K\mu}(\bar{\mathfrak{o}})\mu^{-1}, & \text{if } \mathfrak{n} \text{ is not } K\text{-unary.} \end{cases}$$

and

$$\mu'\bar{\mathfrak{o}} = \begin{cases} \mathfrak{n}, & \text{if } \mathfrak{n} \text{ is } K'\text{-unary;} \\ \Pi_{\Delta\mathfrak{n}/K'\mu'}(\bar{\mathfrak{o}})(\mu')^{-1}, & \text{if } \mathfrak{n} \text{ is not } K'\text{-unary.} \end{cases}$$

Put $\underline{\mu}\bar{\mathfrak{o}} = (\mu\bar{\mathfrak{o}}, \mu'\bar{\mathfrak{o}})$.

**Lemma 4.1.** *For every element $a$ in $K$, we have $a(\mu\bar{\mathfrak{o}}) = (a\mu)\bar{\mathfrak{o}}$.*

*Proof.* First we consider the case when $\mathfrak{n}$ is a $K$-unary prime divisor of $\Delta$. In this case, the stated identity can be written as $a\mathfrak{n} = (a\mathfrak{n})\bar{\mathfrak{o}}$. If $\Delta\mathfrak{n}$ is $K'$-normalized, then $\Delta\mathfrak{n}$ is a finite constants extension of $K'$, and the residue class field of $K$ modulo $\mathfrak{n}$ is contained in the constants field of $\Delta\mathfrak{n}$. On the other hand, we know that the residue class field of $\Delta\mathfrak{n}$ modulo $\bar{\mathfrak{o}}$ contains this constants field as a subfield. That is, modulo $\bar{\mathfrak{o}}$ is the identity map on the constants field. It follows that $(a\mathfrak{n})\bar{\mathfrak{o}} = a\mathfrak{n}$.

When $\mathfrak{n}$ is not $K$-unary, it is clear that $(a\mu)\bar{\mathfrak{o}} = (a\mu)\Pi_{\Delta\mathfrak{n}/K\mu}(\bar{\mathfrak{o}}) = (a\mu)((\mu\bar{\mathfrak{o}})\mu)$ $= a(\mu\bar{\mathfrak{o}})$. □

If $\mathfrak{A}$ is a divisor of $\Delta$, prime to $\mathfrak{n}$, then elements of $[\mathfrak{A}]_{\underline{\mu}\bar{\mathfrak{o}}}$ are $\mathfrak{n}$-integral for every prime divisor $\bar{\mathfrak{o}}$ of $\Delta\mathfrak{n}$. Denote $w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n}) = \min_{a \in [\mathfrak{A}]_{\underline{\mu}\bar{\mathfrak{o}}}} w_{\bar{\mathfrak{o}}}(a\mathfrak{n})$. The **divisor residue** $\mathfrak{A}\mathfrak{n}$ of $\mathfrak{A}$ modulo $\mathfrak{n}$ is defined by

$$\mathfrak{A}\mathfrak{n} = \sum w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n})\bar{\mathfrak{o}} \tag{4.2}$$

where the sum is over all prime divisors $\bar{\mathfrak{o}}$ of $\Delta\mathfrak{n}$. In the following two lemmas we are going to show that the divisor residue $\mathfrak{A}\mathfrak{n}$ is well-defined.

**Lemma 4.3.** *For every prime divisor $\bar{\mathfrak{o}}$ of $\Delta\mathfrak{n}$, $J_{\underline{\mu}\bar{\mathfrak{o}}}\mathfrak{n}$ is contained in the set $\bar{1}_{\bar{\mathfrak{o}}}$ of all $\bar{\mathfrak{o}}$-integral elements in $\Delta\mathfrak{n}$.*

*Proof.* By Lemma 3.2, we have $J_{\underline{\mu}\bar{\mathfrak{o}}} = [1_{\mu\bar{\mathfrak{o}}}, 1'_{\mu'\bar{\mathfrak{o}}}]$. Then $J_{\underline{\mu}\bar{\mathfrak{o}}}\mathfrak{n} = [1_{\mu\bar{\mathfrak{o}}}\mu, 1'_{\mu'\bar{\mathfrak{o}}}\mu']$. It follows from Lemma 4.1 that elements in $1_{\mu\bar{\mathfrak{o}}}\mu$ and $1'_{\mu'\bar{\mathfrak{o}}}\mu'$ are $\bar{\mathfrak{o}}$-integral. Therefore, $J_{\underline{\mu}\bar{\mathfrak{o}}}\mathfrak{n}$ is contained in $\bar{1}_{\bar{\mathfrak{o}}}$. □

**Lemma 4.4.** *Let $\mathfrak{n}$ be a prime divisor of $\Delta$, and let $\mathfrak{A}$ be a divisor of $\Delta$, prime to $\mathfrak{n}$. Then $w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n})$ is finite for every prime divisor $\bar{\mathfrak{o}}$ of $\Delta\mathfrak{n}$, and is zero for almost all prime divisors $\bar{\mathfrak{o}}$ of $\Delta\mathfrak{n}$.*

*Proof.* Since $\mathfrak{A}$ is prime to $\mathfrak{n}$, there exist elements $u$ and $v$ of $\Delta$, prime to $\mathfrak{n}$, such that $uJ_{\underline{\mu}\bar{\mathfrak{o}}} \subseteq [\mathfrak{A}]_{\underline{\mu}\bar{\mathfrak{o}}} \subseteq \frac{1}{v}J_{\underline{\mu}\bar{\mathfrak{o}}}$. Hence, $u\mathfrak{n}J_{\underline{\mu}\bar{\mathfrak{o}}}\mathfrak{n} \subseteq [\mathfrak{A}]_{\underline{\mu}\bar{\mathfrak{o}}}\mathfrak{n} \subseteq \frac{1}{v\mathfrak{n}}J_{\underline{\mu}\bar{\mathfrak{o}}}\mathfrak{n}$. By Lemma 4.3, we have $1 \in J_{\underline{\mu}\bar{\mathfrak{o}}}\mathfrak{n} \subseteq \bar{1}_{\bar{\mathfrak{o}}}$. It follows that $u\mathfrak{n} \in [\mathfrak{A}]_{\underline{\mu}\bar{\mathfrak{o}}}\mathfrak{n} \subseteq \frac{1}{v\mathfrak{n}}\bar{1}_{\bar{\mathfrak{o}}}$. This implies that $w_{\bar{\mathfrak{o}}}(u\mathfrak{n}) \geq w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n}) \geq -w_{\bar{\mathfrak{o}}}(v\mathfrak{n})$. Therefore, $w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n})$ is finite.

Next, there exist elements $u$, $v$ of $\Delta$, prime to $\mathfrak{n}$, such that $uJ \subseteq [\mathfrak{A}] \subseteq \frac{1}{v}J$. If $\bar{\mathfrak{o}}$ is a prime divisor of $\Delta\mathfrak{n}$ such that $\mu\bar{\mathfrak{o}}$, $\mu'\bar{\mathfrak{o}}$ do not occur in $u$, $v$ and $\mathfrak{A}$, then $uJ_{\underline{\mu}\bar{\mathfrak{o}}} \subseteq [\mathfrak{A}]_{\underline{\mu}\bar{\mathfrak{o}}} \subseteq \frac{1}{v}J_{\underline{\mu}\bar{\mathfrak{o}}}$, and hence $w_{\bar{\mathfrak{o}}}(u\mathfrak{n}) \geq w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n}) \geq -w_{\bar{\mathfrak{o}}}(v\mathfrak{n})$. Since there are only finitely many exceptional prime divisors $\bar{\mathfrak{o}}$, $w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n})$ is zero for almost all prime divisors $\bar{\mathfrak{o}}$ of $\Delta\mathfrak{n}$. $\square$

It follows from Lemma 4.4 that the definition of divisor residues is well-defined.

**Lemma 4.5.** *Let $\tilde{K}'$ be a finite extension of $K'$, and let $\mathfrak{n}$ be a prime divisor of $\Delta$. If $\tilde{\mathfrak{n}}$ is a prime divisor of $\tilde{\Delta}$ lying above $\mathfrak{n}$, then $\mathfrak{A}\tilde{\mathfrak{n}} = \mathfrak{A}\mathfrak{n}$ for every divisor $\mathfrak{A}$ of $\Delta$ which is prime to $\mathfrak{n}$.*

*Proof.* Let $\tilde{\mathfrak{o}}$ be any prime divisor of $\tilde{\Delta}\tilde{\mathfrak{n}}$. Then $\bar{\mathfrak{o}} = \Pi_{\tilde{\Delta}\tilde{\mathfrak{n}}/\Delta\mathfrak{n}}(\tilde{\mathfrak{o}})$ is a prime divisor of $\Delta\mathfrak{n}$ lying below $\tilde{\mathfrak{o}}$. Let $\underline{\mu} = (\mu, \mu')$ be the isomorphism pair of $K$, $K'$ induced by $\mathfrak{n}$. It is clear that $a\tilde{\mathfrak{n}} = a\mathfrak{n}$ for every element $a$ in $K$. Thus, $\tilde{\underline{\mu}} = (\mu, \tilde{\mu'})$ is the isomorphism pair of $K$, $\tilde{K}'$ induced by $\tilde{\mathfrak{n}}$ as in Theorem 2.1. It follows that $\mu\tilde{\mathfrak{o}} = \mu\bar{\mathfrak{o}}$. Then, by Theorem 3.3 we have $[\tilde{\mathfrak{A}}]_{\tilde{\underline{\mu}}\tilde{\mathfrak{o}}} = [\mathfrak{A}]_{\mu\bar{\mathfrak{o}}}\tilde{J}_{\tilde{\underline{\mu}}\tilde{\mathfrak{o}}}$. Lemma 4.3 says that $1 \in \tilde{J}_{\tilde{\underline{\mu}}\tilde{\mathfrak{o}}}\tilde{\mathfrak{n}} \subseteq \tilde{1}_{\tilde{\mathfrak{o}}}$. It follows that $w_{\tilde{\mathfrak{o}}}(\mathfrak{A}\tilde{\mathfrak{n}}) = \min_{\tilde{a}\in[\tilde{\mathfrak{A}}]_{\tilde{\underline{\mu}}\tilde{\mathfrak{o}}}} w_{\tilde{\mathfrak{o}}}(\tilde{a}\tilde{\mathfrak{n}}) = \min_{a\in[\mathfrak{A}]_{\underline{\mu}\bar{\mathfrak{o}}}} w_{\tilde{\mathfrak{o}}}(a\tilde{\mathfrak{n}}) = \min_{a\in[\mathfrak{A}]_{\underline{\mu}\bar{\mathfrak{o}}}} w_{\tilde{\mathfrak{o}}}(a\mathfrak{n})$. Let $\bar{\mathfrak{o}} = \sum e_{\tilde{\mathfrak{o}}}\tilde{\mathfrak{o}}$, where $e_{\tilde{\mathfrak{o}}}$ is the ramification index of $\tilde{\mathfrak{o}}$ over $\bar{\mathfrak{o}}$. Then $w_{\tilde{\mathfrak{o}}}(\mathfrak{A}\tilde{\mathfrak{n}}) = e_{\tilde{\mathfrak{o}}}w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n})$. Therefore, $\mathfrak{A}\tilde{\mathfrak{n}} = \sum w_{\tilde{\mathfrak{o}}}(\mathfrak{A}\tilde{\mathfrak{n}})\tilde{\mathfrak{o}} = \sum w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n})\bar{\mathfrak{o}} = \mathfrak{A}\mathfrak{n}$. $\square$

**Lemma 4.6.** *Let $\mathfrak{n}$ be a prime divisor with $\underline{\mu} = (\mu, \mu')$ being the induced isomorphism pair of $K$, $K'$. If $\mathfrak{A}$ is a purely unary divisor of $\Delta$, prime to $\mathfrak{n}$, then $\mathfrak{A}\mathfrak{n}$ is $\mathfrak{A}\mu$ for a $K$-unary divisor $\mathfrak{A}$, and is $\mathfrak{A}\mu'$ for a $K'$-unary divisor $\mathfrak{A}$.*

*Proof.* Let $\mathfrak{A}$ be a $K$-unary divisor, say. If $\bar{\mathfrak{o}}$ is any prime divisor of $\Delta\mathfrak{n}$, then $[\mathfrak{A}]_{\underline{\mu}\bar{\mathfrak{o}}} = [\mathfrak{A}]_{\mu\bar{\mathfrak{o}}}J_{\underline{\mu}\bar{\mathfrak{o}}}$. An element $a$ in $K$ exists such that $[\mathfrak{A}]_{\mu\bar{\mathfrak{o}}} = a1_{\mu\bar{\mathfrak{o}}}$. It follows that $[\mathfrak{A}]_{\underline{\mu}\bar{\mathfrak{o}}} = aJ_{\underline{\mu}\bar{\mathfrak{o}}}$, and hence $[\mathfrak{A}]_{\underline{\mu}\bar{\mathfrak{o}}}\mathfrak{n} = a\mu J_{\underline{\mu}\bar{\mathfrak{o}}}\mathfrak{n}$. By Lemma 4.3, we know that $1 \in J_{\underline{\mu}\bar{\mathfrak{o}}}\mathfrak{n} \subseteq 1_{\bar{\mathfrak{o}}}$. This implies that $w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n}) = w_{\bar{\mathfrak{o}}}(a\mu)$. On the other hand, it can be seen that $w_{\bar{\mathfrak{o}}}(a\mu) = w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mu)$. Therefore, we have $\mathfrak{A}\mathfrak{n} = \mathfrak{A}\mu$. $\square$

Let $\mathfrak{m}$ be a prime divisor of $\Delta$, and let $\mu$, $\mu'$ be the isomorphism pair of $K$, $K'$ induced by $\mathfrak{m}$ as in Theorem 2.1. Then the prime correspondence, which corresponds to every prime divisor $\mathfrak{p}'$ ($\neq \mathfrak{m}$) of $K'$ a divisor $\mathfrak{m}(\mathfrak{p}')$ of $K$, is defined by

$$\mathfrak{m}(\mathfrak{p}') = \begin{cases} \Pi_{\Delta\mathfrak{m}/K\mu}(\mathfrak{p}'\mu')\mu^{-1}, & \text{if } \mathfrak{m} \text{ is binary;} \\ \mathfrak{m}, & \text{if } \mathfrak{m} \text{ is } K\text{-unary;} \\ 0, & \text{if } \mathfrak{m} \text{ is } K'\text{-unary.} \end{cases}$$

**Lemma 4.7.** *Let $\mathfrak{m}$ be a prime divisor of $\Delta$. When $\mathfrak{m}$ is not $K'$-unary, assume that $\Delta\mathfrak{m}$ is $K'$-normalized and that $(\mu, \mu')$ with $\mu' = 1$ is the isomorphism pair of $K$, $K'$ induced by $\mathfrak{m}$. Let $\mathfrak{p}'$ be a $K'$-unary prime divisor, let $\Delta\mathfrak{p}'$ be $K$-normalized, and let $\underline{\pi} = (\pi, \pi')$ with $\pi = 1$ be the isomorphism pair of $K$, $K'$ induced by $\mathfrak{p}'$. If $\mathfrak{m}(\mathfrak{p}')$ is considered as a divisor of $\Delta\mathfrak{p}'$, then $\mathfrak{m}\mathfrak{p}' = \mathfrak{m}(\mathfrak{p}')$.*

*Proof.* When $\mathfrak{m}$ is $K'$-unary, $\mathfrak{m}\mathfrak{p}' = 0 = \mathfrak{m}(\mathfrak{p}')$ by definition. When $\mathfrak{m}$ is $K$-unary, $\mathfrak{m}\mathfrak{p}' = \mathfrak{m}$ by Lemma 4.6, and $\mathfrak{m}(\mathfrak{p}') = \mathfrak{m}$ by definition. Therefore, $\mathfrak{m}\mathfrak{p}' = \mathfrak{m}(\mathfrak{p}')$ for unary prime divisor $\mathfrak{m}$.

For the remaining of the proof, $\mathfrak{m}$ is assumed to be binary. Then the stated identity can be written as

$$\mathfrak{m}\mathfrak{p}' = \Pi_{\Delta\mathfrak{m}/K\mu}(\mathfrak{p}')\mu^{-1} = \mu\mathfrak{p}'.$$

For every prime divisor $\bar{\mathfrak{o}}$ of $\Delta\mathfrak{p}'$, we have $\underline{\pi\bar{\mathfrak{o}}} = (\pi\bar{\mathfrak{o}}, \mathfrak{p}')$. Since $\mathfrak{m}$ is binary, $[\mathfrak{m}]_{\underline{\pi\bar{\mathfrak{o}}}} \subseteq J_{\underline{\pi\bar{\mathfrak{o}}}}$. Furthermore, $a \in [\mathfrak{m}]_{\underline{\pi\bar{\mathfrak{o}}}}$ if, and only if, $a \in J_{\underline{\pi\bar{\mathfrak{o}}}}$ and $a\mathfrak{m} = 0$.

We first consider the case when $\bar{\mathfrak{o}}$ does not divide $\mathfrak{m}(\mathfrak{p}')$, where $\mathfrak{m}(\mathfrak{p}')$ is considered as a divisor of $\Delta\mathfrak{p}'$. Since $[\mathfrak{m}]_{\underline{\pi\bar{\mathfrak{o}}}}\mathfrak{p}' \subseteq J_{\underline{\pi\bar{\mathfrak{o}}}}\mathfrak{p}' \subseteq \bar{1}_{\bar{\mathfrak{o}}}$ by Lemma 4.3, we have $w_{\bar{\mathfrak{o}}}(\mathfrak{m}\mathfrak{p}') \geq 0$. It is clear that an $\pi\bar{\mathfrak{o}}$-integral element $u$ in $K$ exists such that $u(\pi\bar{\mathfrak{o}}) \neq 0$ and $u\mathfrak{m}(\mathfrak{p}') = 0$. By Lemma 4.1, $(u\mu)\mathfrak{p}' = u\mathfrak{m}(\mathfrak{p}') = 0$. It follows that $u\mu$ is $\mathfrak{p}'$-integral, and hence $a = u - u\mu$ belongs to $J_{\underline{\pi\bar{\mathfrak{o}}}}$ and $a\mathfrak{m} = 0$. Thus, $a$ is an element in $[\mathfrak{m}]_{\underline{\pi\bar{\mathfrak{o}}}}$, and $(a\mathfrak{p}')\bar{\mathfrak{o}} = (u\pi - (u\mu)\mathfrak{p}')\bar{\mathfrak{o}} = u(\pi\bar{\mathfrak{o}}) - (u\mathfrak{m}(\mathfrak{p}'))\bar{\mathfrak{o}} = u(\pi\bar{\mathfrak{o}}) \neq 0$. It follows that $w_{\bar{\mathfrak{o}}}(\mathfrak{m}\mathfrak{p}') = 0$.

We now consider the case when $\bar{\mathfrak{o}}$ is a prime divisor of $\Delta\mathfrak{p}'$ dividing $\mathfrak{m}(\mathfrak{p}')$. Then $\pi\bar{\mathfrak{o}} = \mathfrak{m}(\mathfrak{p}')$. By Lemma 3.2 every element $a$ in $J_{\underline{\pi\bar{\mathfrak{o}}}}$ can be written as $a = \sum u_i \cdot u_i'$ with $u_i$ in $1_{\pi\bar{\mathfrak{o}}}$ and $u_i'$ in $1_{\mathfrak{p}'}'$. Then $a\mathfrak{m} = \sum u_i\mu\cdot u_i'$. Since $(u_i\mu)\mathfrak{p}' = u_i\mathfrak{m}(\mathfrak{p}') = u_i(\pi\bar{\mathfrak{o}})$ by Lemma 4.1, the $u_i\mu$ are $\mathfrak{p}'$-integral. Hence $a\mathfrak{m}$ belongs to $J_{\underline{\pi\bar{\mathfrak{o}}}}$. It follows that $[\mathfrak{m}]_{\underline{\pi\bar{\mathfrak{o}}}} = \{a - a\mathfrak{m} : a \in J_{\underline{\pi\bar{\mathfrak{o}}}}\}$. Thus, $w_{\bar{\mathfrak{o}}}(\mathfrak{m}\mathfrak{p}') = \min_{a\in J_{\underline{\pi\bar{\mathfrak{o}}}}} w_{\bar{\mathfrak{o}}}((a - a\mathfrak{m})\mathfrak{p}')$. By Lemma 4.1, $(a - a\mathfrak{m})\mathfrak{p}' = \sum(u_i - u_i\mu)\mathfrak{p}' \cdot u_i'\mathfrak{p}' = \sum(u_i - u_i(\pi\bar{\mathfrak{o}})) \cdot u_i'\pi'$. Since the $u_i'\pi'$ lie in a finite extension of $k$, $w_{\bar{\mathfrak{o}}}(\mathfrak{m}\mathfrak{p}') = w_{\bar{\mathfrak{o}}}(\mathfrak{m}(\mathfrak{p}'))$ when $\bar{\mathfrak{o}}|\mathfrak{m}(\mathfrak{p}')$. Therefore, we have

$$\mathfrak{m}\mathfrak{p}' = \sum w_{\bar{\mathfrak{o}}}(\mathfrak{m}\mathfrak{p}')\bar{\mathfrak{o}} = \sum w_{\bar{\mathfrak{o}}}(\mathfrak{m}(\mathfrak{p}'))\bar{\mathfrak{o}} = \mathfrak{m}(\mathfrak{p}'). \quad \square$$

In the next theorem, we are going to show that divisor residues modulo $\mathfrak{n}$ satisfy the distributive law.

**Theorem 4.8.** *Let $\mathfrak{n}$ be a prime divisor of $\Delta$. If $\mathfrak{A}$ and $\mathfrak{A}_1$ are divisors of $\Delta$, prime to $\mathfrak{n}$, then $(\mathfrak{A} + \mathfrak{A}_1)\mathfrak{n} = \mathfrak{A}\mathfrak{n} + \mathfrak{A}_1\mathfrak{n}$. If $\mathfrak{A}$ is integral or principal, so is $\mathfrak{A}\mathfrak{n}$.*

*Proof.* (1). To prove that $(\mathfrak{A}+\mathfrak{A}_1)\mathfrak{n} = \mathfrak{A}\mathfrak{n}+\mathfrak{A}_1\mathfrak{n}$, it suffices to show that $[\mathfrak{A}+\mathfrak{A}_1]_{\underline{\mathfrak{o}}} = [\mathfrak{A}]_{\underline{\mathfrak{o}}} \cdot [\mathfrak{A}_1]_{\underline{\mathfrak{o}}}$ for every unary pair $\underline{\mathfrak{o}} = (\mathfrak{o}, \mathfrak{o}')$. In fact, for every prime divisor $\bar{\mathfrak{o}}$ of $\Delta\mathfrak{n}$, there exists an element $a$ in $[\mathfrak{A}]_{\underline{\mu\bar{\mathfrak{o}}}}$ and an element $b$ in $[\mathfrak{A}_1]_{\underline{\mu\bar{\mathfrak{o}}}}$ such that $w_{\bar{\mathfrak{o}}}(a\mathfrak{n}) = w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n})$ and $w_{\bar{\mathfrak{o}}}(b\mathfrak{n}) = w_{\bar{\mathfrak{o}}}(\mathfrak{A}_1\mathfrak{n})$. This implies that $w_{\bar{\mathfrak{o}}}((\mathfrak{A} + \mathfrak{A}_1)\mathfrak{n}) \leq w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n}) + w_{\bar{\mathfrak{o}}}(\mathfrak{A}_1\mathfrak{n})$. Conversely, there exists an element $c$ in $[\mathfrak{A} + \mathfrak{A}_1]_{\underline{\mu\bar{\mathfrak{o}}}}$ such that $w_{\bar{\mathfrak{o}}}((\mathfrak{A} + \mathfrak{A}_1)\mathfrak{n}) = w_{\bar{\mathfrak{o}}}(c\mathfrak{n})$. Since $[\mathfrak{A} + \mathfrak{A}_1]_{\underline{\mu\bar{\mathfrak{o}}}} = [\mathfrak{A}]_{\underline{\mu\bar{\mathfrak{o}}}} \cdot [\mathfrak{A}_1]_{\underline{\mu\bar{\mathfrak{o}}}}$, $c = \sum a_ib_i$ with $a_i$ in $[\mathfrak{A}]_{\underline{\mu\bar{\mathfrak{o}}}}$ and $b_i$ in $[\mathfrak{A}_1]_{\underline{\mu\bar{\mathfrak{o}}}}$. It follows that $w_{\bar{\mathfrak{o}}}(c\mathfrak{n}) \geq w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n}) + w_{\bar{\mathfrak{o}}}(\mathfrak{A}_1\mathfrak{n})$. Therefore, $w_{\bar{\mathfrak{o}}}((\mathfrak{A} + \mathfrak{A}_1)\mathfrak{n}) = w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n}) + w_{\bar{\mathfrak{o}}}(\mathfrak{A}_1\mathfrak{n})$. That is, $(\mathfrak{A} + \mathfrak{A}_1)\mathfrak{n} = \mathfrak{A}\mathfrak{n} + \mathfrak{A}_1\mathfrak{n}$.

Now, we are going to prove that $[\mathfrak{A} + \mathfrak{A}_1]_{\underline{\mathfrak{o}}} = [\mathfrak{A}]_{\underline{\mathfrak{o}}} \cdot [\mathfrak{A}_1]_{\underline{\mathfrak{o}}}$ for every unary pair $\underline{\mathfrak{o}}$. Multiplying $\mathfrak{A}$ and $\mathfrak{A}_1$ by suitable nonzero elements of $\Delta$, we can assume that $\mathfrak{A}$ and $\mathfrak{A}_1$ are integral for all binary prime divisors of $\Delta$. First, it is clear that $[\mathfrak{A}]_{\underline{\mathfrak{o}}} \cdot [\mathfrak{A}_1]_{\underline{\mathfrak{o}}} \subseteq [\mathfrak{A} + \mathfrak{A}_1]_{\underline{\mathfrak{o}}}$. Next, by the fundamental theorem of ideal theory of an algebraic function field in [5, Chapter 24], we have $[\mathfrak{A}+\mathfrak{A}_1]_{\mathfrak{o}'} = [\mathfrak{A}]_{\mathfrak{o}'} \cdot [\mathfrak{A}_1]_{\mathfrak{o}'}$ when $\Delta$ is considered as a function field over $K$. Let $\pi$ be a prime element of $\mathfrak{o}$ in $K$. Dividing $\mathfrak{A}$ and $\mathfrak{A}_1$ by some powers of $\pi$, we can assume that $\mathfrak{A}$ and $\mathfrak{A}_1$ are prime to $\mathfrak{o}$. In

order to prove that $[\mathfrak{A}+\mathfrak{A}_1]_{\underline{\mathfrak{o}}} \subseteq [\mathfrak{A}]_{\underline{\mathfrak{o}}} \cdot [\mathfrak{A}_1]_{\underline{\mathfrak{o}}}$, it suffices to show that $a \in [\mathfrak{A}]_{\underline{\mathfrak{o}}} \cdot [\mathfrak{A}_1]_{\underline{\mathfrak{o}}}$ for every element $a \in [\mathfrak{A}+\mathfrak{A}_1]_{\underline{\mathfrak{o}}}$. Since $[\mathfrak{A}+\mathfrak{A}_1]_{\underline{\mathfrak{o}}} \subseteq [\mathfrak{A}+\mathfrak{A}_1]_{\mathfrak{o}'} = [\mathfrak{A}]_{\mathfrak{o}'} \cdot [\mathfrak{A}_1]_{\mathfrak{o}'}$, we can write $a = \sum a_i' \cdot b_i'$ with $a_i' \in [\mathfrak{A}]_{\mathfrak{o}'}$ and $b_i' \in [\mathfrak{A}_1]_{\mathfrak{o}'}$. Then a smallest nonnegative integer $k$ exists such that $\pi^k a = \sum a_i \cdot b_i$ with $a_i \in [\mathfrak{A}]_{\underline{\mathfrak{o}}}$ and $b_i \in [\mathfrak{A}_1]_{\underline{\mathfrak{o}}}$. We want to show that $k=0$.

Argue by contradiction, assuming that $k \geqslant 1$. Let $\eta$ be an element of $[\mathfrak{A}]_{\underline{\mathfrak{o}}}$ such that $w_{\mathfrak{o}'}(\eta\mathfrak{o}) \leqslant w_{\mathfrak{o}'}(a_i\mathfrak{o})$ for each $i$. Put $\bar{\alpha}_i = a_i\mathfrak{o}/\eta\mathfrak{o}$. Then $\bar{\alpha}_i$ is $\mathfrak{o}'$-integral. Since $(a_i - \bar{\alpha}_i\eta)\mathfrak{o} = 0$, we can write $a_i - \bar{\alpha}_i\eta = \pi\bar{c}_i$ for some $\mathfrak{o}$-integral element $\bar{c}_i$. Since $\Delta\mathfrak{o}$ is a finite constants extension of $K'$, we denote by $d$ the degree of $\Delta\mathfrak{o}$ over $K'$. If $\bar{\Delta}$ is the double field of $K$ and $\Delta\mathfrak{o}$, then $\bar{\Delta}$ is a finite extension of $\Delta$ of degree $d$. Let $\alpha_i = \frac{1}{d}\mathrm{trace}_{\bar{\Delta}/\Delta}(\bar{\alpha}_i)$ and $c_i = \frac{1}{d}\mathrm{trace}_{\bar{\Delta}/\Delta}(\bar{c}_i)$. Then $\alpha_i$ is an $\mathfrak{o}'$-integral element of $\Delta$, $c_i$ is an $\mathfrak{o}$-integral element of $\Delta$, and we have $a_i - \alpha_i\eta = \pi c_i$. It is clear that $c_i \in [\mathfrak{A}]_{\underline{\mathfrak{o}}}$. Write $\pi^k a = \pi\sum c_i \cdot b_i + \eta\sum \alpha_i \cdot b_i$. Since $\eta\mathfrak{o} \neq 0$, this identity implies that $\sum \alpha_i \cdot b_i = \pi b$ for some $\mathfrak{o}$-integral element $b$. It is clear that $b \in [\mathfrak{A}_1]_{\underline{\mathfrak{o}}}$. Therefore, we have $\pi^{k-1}a = \sum c_i \cdot b_i + \eta \cdot b$ with $c_i, \eta \in [\mathfrak{A}]_{\underline{\mathfrak{o}}}$ and $b_i, b \in [\mathfrak{A}_1]_{\underline{\mathfrak{o}}}$. This contradicts to the minimality of $k$, and hence we must have $k=0$. Thus, we have proved that $[\mathfrak{A}+\mathfrak{A}_1]_{\underline{\mathfrak{o}}} = [\mathfrak{A}]_{\underline{\mathfrak{o}}} \cdot [\mathfrak{A}_1]_{\underline{\mathfrak{o}}}$.

(2). Assume that $\mathfrak{A}$ is integral. If $\mathfrak{A}_1$ is a divisor of $\Delta$ dividing $\mathfrak{A}$, then for every prime divisor $\bar{\mathfrak{o}}$ of $\Delta\mathfrak{n}$ we have $[\mathfrak{A}]_{\underline{\mu}\bar{\mathfrak{o}}} \subseteq [\mathfrak{A}_1]_{\underline{\mu}\bar{\mathfrak{o}}}$, and hence $[\mathfrak{A}]_{\underline{\mu}\bar{\mathfrak{o}}}\mathfrak{n} \subseteq [\mathfrak{A}_1]_{\underline{\mu}\bar{\mathfrak{o}}}\mathfrak{n}$. This implies that $w_{\bar{\mathfrak{o}}}(\mathfrak{A}\mathfrak{n}) \geq w_{\bar{\mathfrak{o}}}(\mathfrak{A}_1\mathfrak{n})$. That is, $\mathfrak{A}_1\mathfrak{n}$ divides $\mathfrak{A}\mathfrak{n}$. It follows that $\mathfrak{A}\mathfrak{n}$ is integral.

(3). When $\mathfrak{A} = (a)$, by definition we find that $\mathfrak{A}\mathfrak{n} = (a\mathfrak{n})$. Therefore, $\mathfrak{A}\mathfrak{n}$ is principal.

This completes the proof of the theorem.

Finally in this section, we study some properties of general correspondence, which is closely related to divisor residues and will be used in later proofs.

Let $\mathfrak{A} = \sum w_{\mathfrak{m}}(\mathfrak{A})\mathfrak{m}$ be a divisor of $\Delta$, and let $\mathfrak{p}'$ be a prime divisor of $K'$, prime to $\mathfrak{A}$. Then the correspondence $\mathfrak{A}(\mathfrak{p}')$ of $K'$ in $K$ is defined by

$$\mathfrak{A}(\mathfrak{p}') = \sum_{\mathfrak{m}} w_{\mathfrak{m}}(\mathfrak{A})\mathfrak{m}(\mathfrak{p}') \tag{4.9}$$

where the sums are over all prime divisors $\mathfrak{m}$ of $\Delta$.

**Lemma 4.10.** *Let* $\mathfrak{m}$ *be a prime divisor of* $\Delta$*, and let* $\tilde{K}'$ *be a normal splitting extension for* $\mathfrak{m}$*. If* $\tilde{\mathfrak{p}'}$ *is a prime divisor of* $\tilde{K}'$ *lying above a prime divisor* $\mathfrak{p}'$ $(\neq \mathfrak{m})$ *of* $K'$*, then*

$$\mathfrak{m}(\tilde{\mathfrak{p}'}) = \mathfrak{m}(\mathfrak{p}').$$

*Proof.* If $\mathfrak{m}$ is unary, by definition $\mathfrak{m}(\tilde{\mathfrak{p}'}) = \mathfrak{m}(\mathfrak{p}') = \mathfrak{m}$ or $0$. If $\mathfrak{m}$ is binary, assume that $\Delta\mathfrak{m} = K\mu \cdot K'$. Let $\mathfrak{m} = \sum \tilde{\mathfrak{m}}_\sigma$ be the decomposition of $\mathfrak{m}$ as given in Corollary 3.5. We have $\tilde{\Delta}\tilde{\mathfrak{m}}_\sigma = \tilde{K}'$. Let $(\Delta\mathfrak{m})\sigma = K\mu\sigma \cdot K'$. Then the prime divisor $\bar{\mathfrak{p}'}_\sigma$ of $(\Delta\mathfrak{m})\sigma$ containing $\tilde{\mathfrak{p}'}$ is given by

$$\bar{\mathfrak{p}'}_\sigma = \Pi_{\tilde{K}'/(\Delta\mathfrak{m})\sigma}(\tilde{\mathfrak{p}'}).$$

It follows that

$$\tilde{\mathfrak{m}}_\sigma(\tilde{\mathfrak{p}'}) = \Pi_{\tilde{K'}/K\mu\sigma}(\tilde{\mathfrak{p}'})(\mu\sigma)^{-1} = \Pi_{(\Delta\mathfrak{m})\sigma/K\mu\sigma}(\bar{\mathfrak{p}'_\sigma})\sigma^{-1}\mu^{-1}$$
$$= \Pi_{\Delta\mathfrak{m}/K\mu}(\bar{\mathfrak{p}'_\sigma}\sigma^{-1})\mu^{-1}.$$

Since $\sum \bar{\mathfrak{p}'_\sigma}\sigma^{-1} = \mathfrak{p}'$, we have $\mathfrak{m}(\tilde{\mathfrak{p}'}) = \sum_{\underline{\sigma}} \tilde{\mathfrak{m}}_\sigma(\tilde{\mathfrak{p}'}) = \Pi_{\Delta\mathfrak{m}/K\mu}(\sum_{\underline{\sigma}} \bar{\mathfrak{p}'_\sigma}\sigma^{-1})\mu^{-1} = \mathfrak{m}(\mathfrak{p}')$. □

**Theorem 4.11.** *Let $\mathfrak{p}'$ be a prime divisor of $K'$, and let $\underline{\pi} = (\pi, \pi')$ with $\pi = 1$ be the isomorphism pair of $K$, $K'$ induced by $\mathfrak{p}'$. Then for any divisor $\mathfrak{A}$ of $\Delta$, prime to $\mathfrak{p}'$, we have $\mathfrak{A}\mathfrak{p}' = \mathfrak{A}(\mathfrak{p}')$ when $\mathfrak{A}(\mathfrak{p}')$ is considered as a divisor of $\Delta\mathfrak{p}'$.*

*Proof.* By Theorem 4.8 and the definition of general correspondence, we can assume that $\mathfrak{A}$ is a prime divisor $\mathfrak{m}$. Choose $\tilde{K'}$ to be a normal splitting extension of $K'$ for $\mathfrak{m}$. Let $\tilde{\mathfrak{p}'}$ be a prime divisor of $\tilde{K'}$ lying above $\mathfrak{p}'$. Then by Lemma 4.5 and Lemma 4.10 we have $\mathfrak{m}\tilde{\mathfrak{p}'} = \mathfrak{m}\mathfrak{p}'$ and $\mathfrak{m}(\tilde{\mathfrak{p}'}) = \mathfrak{m}(\mathfrak{p}')$. Let $\mathfrak{m} = \sum \tilde{\mathfrak{m}}_\sigma$ be the decomposition of $\mathfrak{m}$ into primes of degree one or zero over $\tilde{K'}$. Then $\mathfrak{m}\tilde{\mathfrak{p}'} = \sum \tilde{\mathfrak{m}}_\sigma\tilde{\mathfrak{p}'}$ and $\mathfrak{m}(\tilde{\mathfrak{p}'}) = \sum \tilde{\mathfrak{m}}_\sigma(\tilde{\mathfrak{p}'})$. It follows from Lemma 4.7 that $\tilde{\mathfrak{m}}_\sigma\tilde{\mathfrak{p}'} = \tilde{\mathfrak{m}}_\sigma(\tilde{\mathfrak{p}'})$, and hence $\mathfrak{m}\tilde{\mathfrak{p}'} = \mathfrak{m}(\tilde{\mathfrak{p}'})$. Consequently, we have $\mathfrak{m}\mathfrak{p}' = \mathfrak{m}(\mathfrak{p}')$. □

**Corollary 4.12.** *Let $\tilde{K'}$ be a finite extension of $K'$, and let $\tilde{\mathfrak{p}'}$ be a prime divisor of $\tilde{K'}$ lying above a prime divisor $\mathfrak{p}'$ of $K'$. Then for any divisor $\mathfrak{A}$ of $\Delta$, prime to $\mathfrak{p}'$, we have $\mathfrak{A}(\tilde{\mathfrak{p}'}) = \mathfrak{A}(\mathfrak{p}')$.*

*Proof.* Let $\underline{\pi} = (\pi, \pi')$ be the isomorphism pair of $K$, $K'$ induced by $\mathfrak{p}'$. By Theorem 4.11, we have $\pi\mathfrak{A}(\tilde{\mathfrak{p}'}) = \mathfrak{A}\tilde{\mathfrak{p}'}$ and $\mathfrak{A}\mathfrak{p}' = \pi\mathfrak{A}(\mathfrak{p}')$. In addition, by Lemma 4.5 we have $\mathfrak{A}\tilde{\mathfrak{p}'} = \mathfrak{A}\mathfrak{p}$. Hence, $\pi\mathfrak{A}(\tilde{\mathfrak{p}'}) = \pi\mathfrak{A}(\mathfrak{p}')$. Since $\pi$ is an isomorphism, $\mathfrak{A}(\tilde{\mathfrak{p}'}) = \mathfrak{A}(\mathfrak{p}')$. □

**Corollary 4.13.** *Let $\mathfrak{p}'$ be a prime divisor of $K'$, and let $\mathfrak{A}$, $\mathfrak{A}_1$ and $\mathfrak{A}_2$ be divisors of $\Delta$, prime to $\mathfrak{p}'$. Then*

*(1).* $(\mathfrak{A}_1 + \mathfrak{A}_2)(\mathfrak{p}') = \mathfrak{A}_1(\mathfrak{p}') + \mathfrak{A}_2(\mathfrak{p}')$.

*(2). If $\mathfrak{A}$ is integral or principal, so is $\mathfrak{A}(\mathfrak{p}')$.*

*(3).*

$$\mathfrak{A}(\mathfrak{p}') = \begin{cases} \mathfrak{A}, & \text{if } \mathfrak{A} \text{ is } K\text{-unary;} \\ 0, & \text{if } \mathfrak{A} \text{ is } K'\text{-unary.} \end{cases}$$

*Proof.* We have (1) and (2) by Theorem 4.11 and Theorem 4.8 , and we have (3) by (1) and the definition of correspondence. □

## 5. Norm of divisor residues

In this section, we prove a theorem about the norm of divisor residues, which is essential for our definition of a residue scalar product for algebraic function fields over number fields.

Assume that $L$ is a finite separable extension of $F$, and let $\mathfrak{P}$ be a prime divisor of $L$. Define

$$\mathfrak{N}_{L/F}(\mathfrak{P}) = \sum_\sigma \mathfrak{P}\sigma$$

where the sum is over all isomorphisms of $L$ over $F$. We extend the map $\mathfrak{N}_{L/F}$ to the group of all divisors of $L$ by additivity.

**Lemma 5.1.** *Let* $\mathfrak{m}$ *and* $\mathfrak{n}$ *be different binary prime divisors of* $\Delta$, *and let* $\underline{\pi} = (\pi, \pi')$ *be the isomorphism pair of* $K$, $K'$ *induced by* $\mathfrak{n}$. *If* $\bar{\mathfrak{o}}$ *is a prime divisor of* $\Delta\mathfrak{n}$, *then* $\bar{\mathfrak{o}}|\mathfrak{mn}$ *if, and only if,* $\pi\bar{\mathfrak{o}}|\mathfrak{m}(\pi'\bar{\mathfrak{o}})$.

*Proof.* Denote $\mathfrak{o} = \pi\bar{\mathfrak{o}}$ and $\mathfrak{o}' = \pi'\bar{\mathfrak{o}}$. Then $\mathfrak{o}$ and $\mathfrak{o}'$ are unary prime divisors. Moreover, $\mathfrak{o}$ divides $\mathfrak{m}(\mathfrak{o}')$ if, and only if, $\mathfrak{o}\mu$ divides $\Pi_{\Delta\mathfrak{m}/K\mu}(\mathfrak{o}'\mu')$, where $\underline{\mu} = (\mu, \mu')$ is the isomorphism pair of $K$, $K'$ induced by $\mathfrak{m}$. Since $\mathfrak{o}\mu$ is a prime divisor in $K\mu$, $\mathfrak{o}\mu$ divides $\Pi_{\Delta\mathfrak{m}/K\mu}(\mathfrak{o}'\mu')$ if, and only if, $\mathfrak{o}\mu$ and $\mathfrak{o}'\mu'$ are not coprime in $\Delta\mathfrak{m}$.

We first consider the case when $\mathfrak{o}$ divides $\mathfrak{m}(\mathfrak{o}')$. Let $\bar{\mathfrak{o}_{\mathfrak{m}}}$ be a common prime divisor of $\mathfrak{o}\mu$ and $\mathfrak{o}'\mu'$ in $\Delta\mathfrak{m}$. Then $\underline{\mu}\bar{\mathfrak{o}_{\mathfrak{m}}} = (\mathfrak{o}, \mathfrak{o}')$. Since $\mathfrak{m}$ is a binary prime divisor, $[\mathfrak{m}]_{\underline{\pi}\bar{\mathfrak{o}}}$ is the set of all elements $a$ in $J_{\underline{\pi}\bar{\mathfrak{o}}}$ such that $a\mathfrak{m} = 0$. Now, for every element $a = \sum u_i \cdot u_i'$ in $[\mathfrak{m}]_{\underline{\pi}\bar{\mathfrak{o}}}$ with $u_i \in 1_{\pi\bar{\mathfrak{o}}}$ and $u_i' \in 1'_{\pi'\bar{\mathfrak{o}}}$, we have $(a\mathfrak{n})\bar{\mathfrak{o}} = \sum(u_i\pi)\bar{\mathfrak{o}} \cdot (u_i'\pi')\bar{\mathfrak{o}} = \sum u_i\mathfrak{o} \cdot u_i'\mathfrak{o}' = \sum u_i(\mu\bar{\mathfrak{o}_{\mathfrak{m}}}) \cdot u_i'(\mu'\bar{\mathfrak{o}_{\mathfrak{m}}}) = (a\mathfrak{m})\bar{\mathfrak{o}_{\mathfrak{m}}} = 0$. It follows that $w_{\bar{\mathfrak{o}}}(\mathfrak{mn}) \geq 1$. That is, $\bar{\mathfrak{o}}$ divides $\mathfrak{mn}$.

We now consider the case when $\mathfrak{o}$ does not divide $\mathfrak{m}(\mathfrak{o}')$. Then $\mathfrak{o}\mu$ and $\mathfrak{o}'\mu'$ are coprime. It follows that an element $u$ in $K$ exists such that $u\mu \equiv 1$ modulo $\mathfrak{o}\mu$ and $u\mu \equiv 0$ modulo $\mathfrak{o}'\mu'$. Assume that $x^k + a_1x^{k-1} + \cdots + a_k$ be the irreducible generating polynomial of $\Delta\mathfrak{m}$ over $K'\mu'$. Define $\underline{u} = (u^k, \cdots, u, 1)$ and $\underline{u'} = (1, a_1, \cdots, a_k)(\mu')^{-1}$. Then $\underline{u}\mu \cdot \underline{u'}\mu' = 0$. Since $u\mu \equiv 1$ modulo $\mathfrak{o}\mu$ and $u\mu \equiv 0$ modulo $\mathfrak{o}'\mu'$, we have $\underline{u}\mathfrak{o} = (1, 1, \cdots, 1)$ and $\underline{u'}\mathfrak{o}' = (1, 0, \cdots, 0)$. Let $a = \underline{u} \cdot \underline{u'}$. Then $a$ belongs to $[\mathfrak{m}]_{\underline{\pi}\bar{\mathfrak{o}}}$. Moreover, $(a\mathfrak{n})\bar{\mathfrak{o}} = \underline{u}\mathfrak{o} \cdot \underline{u'}\mathfrak{o}' = 1$. This implies that $w_{\bar{\mathfrak{o}}}(\mathfrak{mn}) = 0$, and therefore, $\bar{\mathfrak{o}}$ does not divide $\mathfrak{mn}$. □

Let $\underline{\mu} = (\mu_1, \mu_2)$ be a pair of different isomorphisms of $K$ into an algebraic function field. Denote $\tilde{K}' = K\mu_1 \cdot K\mu_2$ the field composite of $K\mu_1$ and $K\mu_2$. For every prime divisor $\tilde{\mathfrak{o}}$ of $\tilde{K}'$, define $\ell_{\tilde{\mathfrak{o}}} = \min_{a \in 1_{\underline{\mu}\tilde{\mathfrak{o}}}} w_{\tilde{\mathfrak{o}}}(a\mu_1 - a\mu_2)$, where $\underline{\mu}\tilde{\mathfrak{o}} = (\mu_1\tilde{\mathfrak{o}}, \mu_2\tilde{\mathfrak{o}})$ and $1_{\underline{\mu}\tilde{\mathfrak{o}}}$ is the set of all elements in $K$ which are integral for $\mu_1\tilde{\mathfrak{o}}$ and $\mu_2\tilde{\mathfrak{o}}$. A different divisor $\mathfrak{D}_{\underline{\mu}}$ for the isomorphism pair $\underline{\mu}$ is defined by

$$\mathfrak{D}_{\underline{\mu}} = \sum_{\tilde{\mathfrak{o}}} \ell_{\tilde{\mathfrak{o}}}\tilde{\mathfrak{o}}$$

where the sum is over all prime divisors $\tilde{\mathfrak{o}}$ of $\tilde{K}'$. In general, if $\underline{\mu} = (\mu_1, \cdots, \mu_n)$ is a system of different isomorphisms of $K$ into an algebraic function field, then the conjugate different divisors $\mathfrak{D}_{\underline{\mu}}^{(i)}$ are defined by

$$\mathfrak{D}_{\underline{\mu}}^{(i)} = \sum_{j=1, j\neq i}^{m} \mathfrak{D}_{\mu_i, \mu_j}$$

for $i = 1, 2, \cdots, n$, and the discriminant divisor $\mathfrak{D}_{\underline{\mu}}$ is then defined by

$$\mathfrak{D}_{\underline{\mu}} = \sum_{i=1}^{m} \mathfrak{D}_{\underline{\mu}}^{(i)}.$$

**Lemma 5.2.** *Let $\mathfrak{m}$ and $\mathfrak{n}$ be two different prime divisors of $\Delta$, which are not $K'$-unary. Assume that $\Delta\mathfrak{m} = K\mu_0 \cdot K'$ and $\Delta\mathfrak{n} = K\nu \cdot K'$. If $\underline{\mu}$ is the isomorphism system of $K$ coordinated to $\mu_0$, then*

$$\mathfrak{m}\mathfrak{n} = \sum_{\mu \in \underline{\mu}} \mathfrak{D}_{\mu,\nu}$$

*where the sum is over all isomorphisms in the isomorphism system $\underline{\mu}$.*

*Proof.* Assume that $\tilde{K}'$ is a splitting extension of $K'$ for $\mathfrak{m}$ which contains $K\nu$. Since $\mathfrak{m}$ and $\mathfrak{n}$ are different prime divisors of $\Delta$, by Theorem 2.1 $\mu$ is not equal to $\nu$ for every isomorphism $\mu$ in $\underline{\mu}$.

(1). We first consider the case when $\mathfrak{m}$ and $\mathfrak{n}$ are binary prime divisors of $\Delta$ with $N_{\Delta/K'}(\mathfrak{m}) = 1$. In this case, $\underline{\mu}$ consists of a single isomorphism $\mu$, and $K\mu \subseteq \Delta\mathfrak{m} = K' \subseteq \Delta\mathfrak{n} = K\nu \cdot K'$. Hence, we can choose $\tilde{K}' = \Delta\mathfrak{n}$ by the argument preceding the statement of Lemma 3.4. The stated identity can then be written as

$$w_{\bar{\mathfrak{o}}}(\mathfrak{m}\mathfrak{n}) = w_{\bar{\mathfrak{o}}}(\mathfrak{D}_{\mu,\nu})$$

for every prime divisor $\bar{\mathfrak{o}}$ of $\Delta\mathfrak{n}$.

Assume that $\mu\bar{\mathfrak{o}}$ is not equal to $\nu\bar{\mathfrak{o}}$. Then $w_{\bar{\mathfrak{o}}}(\mathfrak{D}_{\mu,\nu}) = 0$ by definition. In order to see that $w_{\bar{\mathfrak{o}}}(\mathfrak{m}\mathfrak{n}) = 0$, it suffices to show that $\nu\bar{\mathfrak{o}}$ does not divide $\mathfrak{m}(\nu'\bar{\mathfrak{o}})$ by Lemma 5.1, where $\nu$, $\nu'$ with $\nu' = 1$ is the isomorphism pair of $K$, $K'$ induced by $\mathfrak{n}$. We have $\mathfrak{m}(\nu'\bar{\mathfrak{o}}) = \Pi_{\Delta\mathfrak{m}/K\mu}(\nu'\bar{\mathfrak{o}})\mu^{-1}$. Since $\nu'\bar{\mathfrak{o}} = \Pi_{\Delta\mathfrak{n}/K'}(\bar{\mathfrak{o}})$, we have $\mathfrak{m}(\nu'\bar{\mathfrak{o}}) = \Pi_{\Delta\mathfrak{n}/K\mu}(\bar{\mathfrak{o}})\mu^{-1} = \mu\bar{\mathfrak{o}}$. Since $\mu\bar{\mathfrak{o}} \neq \nu\bar{\mathfrak{o}}$ by assumption, we have $\nu\bar{\mathfrak{o}}$ does not divide $\mathfrak{m}(\nu'\bar{\mathfrak{o}})$.

Next, assume that $\mu\bar{\mathfrak{o}} = \nu\bar{\mathfrak{o}}$. Denote $\mathfrak{o} = \mu\bar{\mathfrak{o}} = \nu\bar{\mathfrak{o}}$. If $u$ is integral for $\mathfrak{o}$, then $u\mu$ is integral for $\mathfrak{o}\mu = \Pi_{\Delta\mathfrak{n}/K\mu}(\bar{\mathfrak{o}}) = \Pi_{K'/K\mu}(\nu'\bar{\mathfrak{o}})$. This implies that $u\mu$ is integral for $\nu'\bar{\mathfrak{o}}$. Hence, elements of the form $u - u\mu$ with $u$ in $1_{\mathfrak{o}}$ belongs to $[\mathfrak{m}]_{\underline{\mathfrak{o}}}$ by Lemma 3.2, where $\underline{\mathfrak{o}} = (\mathfrak{o}, \nu'\bar{\mathfrak{o}})$. Since $\mathfrak{m}$ is a binary prime divisor, $[\mathfrak{m}]_{\underline{\mathfrak{o}}}$ is the set of elements $a$ in $J_{\underline{\mathfrak{o}}}$ such that $a\mathfrak{m} = 0$. If $a$ belongs to $[\mathfrak{m}]_{\underline{\mathfrak{o}}}$, then $a = \underline{u} \cdot \underline{u'}$ and $a\mathfrak{m} = 0$ with $\underline{u}$, $\underline{u'}$ being vectors of equal length over $1_{\mathfrak{o}}$, $1_{\nu'\bar{\mathfrak{o}}}$, and hence $a = \underline{u}\cdot\underline{u'} - \underline{u}\mu\cdot\underline{u'} = (\underline{u} - \underline{u}\mu)\cdot\underline{u'}$. It follows that $[\mathfrak{m}]_{\underline{\mathfrak{o}}}$ is generated over $1'_{\nu'\bar{\mathfrak{o}}}$ by elements of the form $u - u\mu$ with $u$ in $1_{\mathfrak{o}}$. This implies that

$$w_{\bar{\mathfrak{o}}}(\mathfrak{m}\mathfrak{n}) = \min_{u \in 1_{\mathfrak{o}}}(u\mu - u\nu)$$

by the definition of divisor residues. Therefore, by the definition of different divisors we have

$$w_{\bar{\mathfrak{o}}}(\mathfrak{m}\mathfrak{n}) = w_{\bar{\mathfrak{o}}}(\mathfrak{D}_{\mu,\nu}).$$

Thus, we have verified the stated identity in the case when $\mathfrak{m}$ and $\mathfrak{n}$ are binary prime divisors of $\Delta$ with $N_{\Delta/K'}(\mathfrak{m}) = 1$.

(2). We now consider the general case when $\mathfrak{m}$ and $\mathfrak{n}$ are binary prime divisors of $\Delta$ with $N_{\Delta/K'}(\mathfrak{m})$ arbitrary. Let $\tilde{K}'$ be a splitting extension for $\mathfrak{m}$, which contains $K\nu$. Then, by Corollary 3.5, $\mathfrak{m}$ has in the double field $\tilde{\Delta}$ of $K$ and $\tilde{K}'$ the decomposition

$$\mathfrak{m} = \sum_{\underline{\mu}} \tilde{\mathfrak{m}}_{\mu}$$

into prime divisors $\tilde{\mathfrak{m}}_\mu$ with $N_{\tilde{\Delta}/\tilde{K'}}(\tilde{\mathfrak{m}}_\mu) = 1$. Let $\tilde{\mathfrak{n}}$ be a prime divisor of $\tilde{\Delta}$ lying above $\mathfrak{n}$. By Lemma 4.5, we have $\mathfrak{m}\mathfrak{n} = \mathfrak{m}\tilde{\mathfrak{n}}$. By using Theorem 4.8, we obtain that

$$\mathfrak{m}\mathfrak{n} = \sum_{\underline{\mu}} \tilde{\mathfrak{m}}_\mu \tilde{\mathfrak{n}}.$$

Note that $\tilde{\mathfrak{n}}$ and $\mathfrak{n}$ induce the same isomorphism $\nu$ of $K$ into $\tilde{K'}$. By the first part of the proof we have

$$\tilde{\mathfrak{m}}_\mu \tilde{\mathfrak{n}} = \mathfrak{D}_{\mu,\nu}$$

for every isomorphism $\mu$ in $\underline{\mu}$, and hence

$$\mathfrak{m}\mathfrak{n} = \sum_{\underline{\mu}} \mathfrak{D}_{\mu,\nu}.$$

(3). We finally consider the case when one of $\mathfrak{m}$ and $\mathfrak{n}$ is a $K$-unary prime divisor. Assume first that $\mathfrak{m}$ is a $K$-unary prime divisor, then by Lemma 4.6 $\mathfrak{m}\mathfrak{n} = \mathfrak{m}\nu$. On the other hand, we have $\mu\bar{\mathfrak{o}} = \mathfrak{m}$. When $\mathfrak{n}$ is $K$-unary, we have $\nu\bar{\mathfrak{o}} = \mathfrak{n}$, and hence $\mathfrak{D}_{\mu,\nu} = 0$. When $\mathfrak{n}$ is $K$-unary, we also have $\mathfrak{m}\mathfrak{n} = 0$ by the definition of divisor residues, and therefore $\mathfrak{m}\mathfrak{n} = \mathfrak{D}_{\mu,\nu}$. When $\mathfrak{n}$ is binary, we have $\nu\bar{\mathfrak{o}} = \Pi_{\Delta\mathfrak{n}/K\nu}(\bar{\mathfrak{o}})\nu^{-1}$. It follows from definition that $\mathfrak{D}_{\mu,\nu} = \mathfrak{m}\nu$. Therefore, we have $\mathfrak{m}\mathfrak{n} = \mathfrak{D}_{\mu,\nu}$.

Next, assume that $\mathfrak{n}$ is $K$-unary and that $\mathfrak{m}$ is binary. Since $\mathfrak{m}\mathfrak{n} = \mathfrak{m}(\mathfrak{n})$ by Theorem 4.11 (with the role of $K$ and $K'$ being interchanged), we have $\mathfrak{m}\mathfrak{n} = \Pi_{\Delta\mathfrak{m}/K'}(\mathfrak{n}\mu_0)$. On the other hand, we have $\mathfrak{D}_{\mu,\nu} = \mathfrak{n}\mu$ for every isomorphism $\mu$ in $\underline{\mu}$. Hence, we have

$$\sum_{\mu\in\underline{\mu}} \mathfrak{D}_{\mu,\nu} = \sum_{\mu\in\underline{\mu}} \mathfrak{n}\mu = \Pi_{\Delta\mathfrak{m}/K'}(\mathfrak{n}\mu_0) = \mathfrak{m}\mathfrak{n}$$

by considering first the case when $N_{\Delta/K'}(\mathfrak{m}) = 1$ and then the case when $N_{\Delta/K'}(\mathfrak{m})$ is arbitrary. $\square$

In the following theorem, we take the norm of divisor residues.

**Theorem 5.3.** *Let $\mathfrak{m}$ and $\mathfrak{n}$ be two different prime divisors of $\Delta$, and let $(\mu, \mu')$ and $(\nu, \nu')$ be the isomorphism pairs of $K'$ induced by $\mathfrak{m}$ and $\mathfrak{n}$, respectively. If $\mathfrak{m}$ is a $K'$-unary prime divisor, define $\mathfrak{N}_{\Delta\mathfrak{m}/K'\mu'}(\mathfrak{n}\mathfrak{m})\mu'^{-1} = N_{\Delta/K'}(\mathfrak{n})\mathfrak{m}$, and if $\mathfrak{n}$ is a $K'$-unary prime divisor, define $\mathfrak{N}_{\Delta\mathfrak{n}/K'\nu'}(\mathfrak{m}\mathfrak{n})\nu'^{-1} = N_{\Delta/K'}(\mathfrak{m})\mathfrak{n}$, then*

$$\mathfrak{N}_{\Delta\mathfrak{m}/K'\mu'}(\mathfrak{n}\mathfrak{m})\mu'^{-1} = \mathfrak{N}_{\Delta\mathfrak{n}/K'\nu'}(\mathfrak{m}\mathfrak{n})\nu'^{-1}.$$

*If $\mathfrak{m}$ is a $K$-unary prime divisor, define $\mathfrak{N}_{\Delta\mathfrak{m}/K\mu}(\mathfrak{n}\mathfrak{m})\mu^{-1} = N_{\Delta/K}(\mathfrak{n})\mathfrak{m}$, and if $\mathfrak{n}$ is a $K$-unary prime divisor, define $\mathfrak{N}_{\Delta\mathfrak{n}/K\nu}(\mathfrak{m}\mathfrak{n})\nu^{-1} = N_{\Delta/K}(\mathfrak{m})\mathfrak{n}$, then*

$$\mathfrak{N}_{\Delta\mathfrak{m}/K\mu}(\mathfrak{n}\mathfrak{m})\mu^{-1} = \mathfrak{N}_{\Delta\mathfrak{n}/K\nu}(\mathfrak{m}\mathfrak{n})\nu^{-1}.$$

*Proof.* We first consider the case when $\mathfrak{m}$ and $\mathfrak{n}$ are not $K'$-unary. Assume that $\Delta\mathfrak{m} = K\mu_0 \cdot K'$ and $\Delta\mathfrak{n} = K\nu_0 \cdot K'$. Let $\underline{\mu}$, $\underline{\nu}$ be isomorphism systems of $K$ coordinated to $\mu_0$, $\nu_0$. By Lemma 5.2 we have $\mathfrak{m}\mathfrak{n} = \sum_{\mu\in\underline{\mu}} \mathfrak{D}_{\mu,\nu_0}$. If $\sigma$ is an isomorphism of $\Delta\mathfrak{n}$ over $K'$, then $(\mathfrak{m}\mathfrak{n})\sigma = \sum_{\mu\in\underline{\mu}} \mathfrak{D}_{\mu,\nu_0\sigma}$. It follows that

$$\mathfrak{N}_{\Delta\mathfrak{n}/K'}(\mathfrak{m}\mathfrak{n}) = \sum_{\mu\in\underline{\mu},\nu\in\underline{\nu}} \mathfrak{D}_{\mu,\nu}.$$

Since $\mathfrak{D}_{\mu,\nu} = \mathfrak{D}_{\nu,\mu}$, we have

$$\mathfrak{N}_{\Delta\mathfrak{n}/K'}(\mathfrak{m}\mathfrak{n}) = \mathfrak{N}_{\Delta\mathfrak{m}/K'}(\mathfrak{n}\mathfrak{m}).$$

This implies that

$$\mathfrak{N}_{\Delta\mathfrak{m}/K'\mu'}(\mathfrak{n}\mathfrak{m}){\mu'}^{-1} = \mathfrak{N}_{\Delta\mathfrak{n}/K'\nu'}(\mathfrak{m}\mathfrak{n}){\nu'}^{-1}$$

when $\Delta\mathfrak{n}$ and $\Delta\mathfrak{m}$ are not $K'$-normalized. When $\mathfrak{m}$ and $\mathfrak{n}$ are not $K$-unary, a similar argument shows that the identity

$$\mathfrak{N}_{\Delta\mathfrak{m}/K\mu}(\mathfrak{n}\mathfrak{m})\mu^{-1} = \mathfrak{N}_{\Delta\mathfrak{n}/K\nu}(\mathfrak{m}\mathfrak{n})\nu^{-1}$$

holds.

We now consider the case when one of $\mathfrak{m}$ and $\mathfrak{n}$ is $K'$-unary, say $\mathfrak{m}$. Then $\mathfrak{N}_{\Delta\mathfrak{m}/K'\mu'}(\mathfrak{n}\mathfrak{m}){\mu'}^{-1} = N_{\Delta/K'}(\mathfrak{n})\mathfrak{m}$ by assumption. If $\mathfrak{n}$ is not $K'$-unary, then by Lemma 4.6 we have $\mathfrak{m}\mathfrak{n} = \mathfrak{m}\nu'$. It follows that $\mathfrak{N}_{\Delta\mathfrak{n}/K'\nu'}(\mathfrak{m}\mathfrak{n}){\nu'}^{-1} = [\Delta\mathfrak{n} : K'\nu']\mathfrak{m} = N_{\Delta/K'}(\mathfrak{n})\mathfrak{m}$. Therefore,

$$\mathfrak{N}_{\Delta\mathfrak{m}/K'\mu'}(\mathfrak{n}\mathfrak{m}){\mu'}^{-1} = \mathfrak{N}_{\Delta\mathfrak{n}/K'\nu'}(\mathfrak{m}\mathfrak{n}){\nu'}^{-1}$$

when $\mathfrak{n}$ is not a $K'$-unary prime divisor. If $\mathfrak{n}$ is $K'$-unary, then $N_{\Delta/K'}(\mathfrak{n}) = 0$ and $N_{\Delta/K'}(\mathfrak{m}) = 0$ by definition. Since $\mathfrak{N}_{\Delta\mathfrak{n}/K'\nu'}(\mathfrak{m}\mathfrak{n}){\nu'}^{-1} = N_{\Delta/K'}(\mathfrak{m})\mathfrak{n}$ by assumption, we have

$$\mathfrak{N}_{\Delta\mathfrak{m}/K'\mu'}(\mathfrak{n}\mathfrak{m}){\mu'}^{-1} = \mathfrak{N}_{\Delta\mathfrak{n}/K'\nu'}(\mathfrak{m}\mathfrak{n}){\nu'}^{-1} = 0$$

when $\mathfrak{n}$ is a $K'$-unary prime divisor.

We finally consider the case when one of $\mathfrak{m}$ and $\mathfrak{n}$ is $K$-unary, say $\mathfrak{n}$. Then $\mathfrak{N}_{\Delta\mathfrak{n}/K\nu}(\mathfrak{m}\mathfrak{n})\nu^{-1} = N_{\Delta/K}(\mathfrak{m})\mathfrak{n}$ by assumption. If $\mathfrak{m}$ is not $K$-unary, then by Lemma 4.6 we have $\mathfrak{n}\mathfrak{m} = \mathfrak{n}\mu$. It follows that

$$\mathfrak{N}_{\Delta\mathfrak{m}/K\mu}(\mathfrak{n}\mathfrak{m})\mu^{-1} = [\Delta\mathfrak{m} : K\mu]\mathfrak{n} = N_{\Delta/K}(\mathfrak{m})\mathfrak{n}.$$

Therefore,

$$\mathfrak{N}_{\Delta\mathfrak{m}/K\mu}(\mathfrak{n}\mathfrak{m})\mu^{-1} = \mathfrak{N}_{\Delta\mathfrak{n}/K\nu}(\mathfrak{m}\mathfrak{n})\nu^{-1}$$

when $\mathfrak{m}$ is not a $K$-unary prime divisor. If $\mathfrak{m}$ is $K$-unary, then $N_{\Delta/K}(\mathfrak{m}) = 0$ and $N_{\Delta/K}(\mathfrak{n}) = 0$ by definition. Since $\mathfrak{N}_{\Delta\mathfrak{m}/K\mu}(\mathfrak{n}\mathfrak{m})\mu^{-1} = N_{\Delta/K}(\mathfrak{n})\mathfrak{m}$ by assumption, we have

$$\mathfrak{N}_{\Delta\mathfrak{m}/K\mu}(\mathfrak{n}\mathfrak{m})\mu^{-1} = \mathfrak{N}_{\Delta\mathfrak{n}/K\nu}(\mathfrak{m}\mathfrak{n})\nu^{-1} = 0$$

when $\mathfrak{n}$ is a $K$-unary prime divisor.

This completes the proof of the theorem.

Let $\mathfrak{A}$ and $\mathfrak{b}$ be divisors of $\Delta$, relatively prime to each other. Write $\mathfrak{A} = \sum a_{\mathfrak{m}}\mathfrak{m}$ and $\mathfrak{b} = \sum b_{\mathfrak{n}}\mathfrak{n}$ as linear combination of prime divisors of $\Delta$ with integer coefficients. Define

$$\langle \mathfrak{A}, \mathfrak{b}\rangle_f = \sum_{\mathfrak{m},\mathfrak{n}} a_{\mathfrak{m}} b_{\mathfrak{n}} \mathfrak{N}_{\Delta\mathfrak{n}/K\nu}(\mathfrak{m}\mathfrak{n})\nu^{-1}$$

and

$$\langle \mathfrak{A}, \mathfrak{b}\rangle'_f = \sum_{\mathfrak{m},\mathfrak{n}} a_{\mathfrak{m}} b_{\mathfrak{n}} \mathfrak{N}_{\Delta\mathfrak{n}/K'\nu'}(\mathfrak{m}\mathfrak{n}){\nu'}^{-1}. \tag{5.4}$$

Note that $\langle \mathfrak{A}, \mathfrak{b}\rangle_f$ is a divisor of $K$ and that $\langle \mathfrak{A}, \mathfrak{b}\rangle'_f$ is a divisor of $K'$. It follows from Theorem 5.3 that $\langle \mathfrak{A}, \mathfrak{b}\rangle_f = \langle \mathfrak{b}, \mathfrak{A}\rangle_f$ and $\langle \mathfrak{A}, \mathfrak{b}\rangle'_f = \langle \mathfrak{b}, \mathfrak{A}\rangle'_f$.

**Lemma 5.5.** *Let $\mathfrak{m}$ be a binary prime divisor of $\Delta$ with $N_{\Delta/K'}(\mathfrak{m}) = 1$. Assume that $x$ is a separating element of $K$. Denote by $dx$ the divisor $\mathfrak{D}_x/u_x^2$, where $\mathfrak{D}_x$ is the different of $K$ over $k(x)$ and $u_x$ is the denominator of $x$. Then $\langle \mathfrak{m}, \mathfrak{m}\rangle_f + \langle dx, \mathfrak{m}\rangle_f$ and $\langle \mathfrak{m}, \mathfrak{m}\rangle'_f + \langle dx, \mathfrak{m}\rangle'_f$ are principal.*

*Proof.* Denote by $\mu$, $\mu'$ the isomorphism pair of $K$, $K'$ induced by $\mathfrak{m}$. Assume that $\Delta\mathfrak{m}$ is $K'$-normalized. Since $N_{\Delta/K'}(\mathfrak{m}) = 1$, we have $K\mu \subseteq \Delta\mathfrak{m} = K'$. Since $x$ is an separating element of $K$, it is integral for $\mathfrak{m}$, and $x - x\mu \equiv 0$ modulo $\mathfrak{m}$. Denote by $\mathfrak{m}_0$ the numerator of $x - x\mu$. Then $\mathfrak{m}_0$ is a prime divisor of $K'(x)$ of $K'$-degree one, which is not a prime divisor of $k(x)$. Hence, $\mathfrak{m}_0$ is not contained in the discriminant of $\Delta/K'(x)$, which consists of only prime divisors of $k(x)$. It follows that $\mathfrak{m}_0$ is unramified in $\Delta$ over $K'(x)$. This implies that $\mathfrak{m}_0$ contains $\mathfrak{m}$ only once. It follows that there exists a divisor $\mathfrak{n}$, prime to $\mathfrak{m}$, such that $(x - x\mu) = \mathfrak{m} - \mathfrak{n}$. By Theorem 4.8, $\langle \mathfrak{m}, \mathfrak{m}\rangle_f - \langle \mathfrak{n}, \mathfrak{m}\rangle_f$ and $\langle \mathfrak{m}, \mathfrak{m}\rangle'_f - \langle \mathfrak{n}, \mathfrak{m}\rangle'_f$ are principal. Thus, the stated result is equivalent to the statement that $\langle \mathfrak{m}, \mathfrak{m}\rangle_f + \langle dx, \mathfrak{m}\rangle_f$ and $\langle \mathfrak{m}, \mathfrak{m}\rangle'_f + \langle dx, \mathfrak{m}\rangle'_f$ are principal. Since $\Delta\mathfrak{m} = K'$ and since $dx$ is $K$-unary, by Lemma 4.6 we have

$$\begin{aligned}\langle \mathfrak{n}, \mathfrak{m}\rangle_f + \langle dx, \mathfrak{m}\rangle_f &= \mathfrak{N}_{K'/K\mu}(\mathfrak{n}\mathfrak{m})\mu^{-1} + \mathfrak{N}_{K'/K\mu}((dx)\mu)\mu^{-1}\\ &= \mathfrak{N}_{K'/K\mu}\left(\mathfrak{n}\mathfrak{m} + (dx)\mu\right)\mu^{-1}\end{aligned}$$

and

$$\langle \mathfrak{n}, \mathfrak{m}\rangle'_f + \langle dx, \mathfrak{m}\rangle'_f = \mathfrak{n}\mathfrak{m} + (dx)\mu.$$

Therefore, it suffices to show that $\mathfrak{n}\mathfrak{m} + (dx)\mu$ is principal.

Let $\tilde{K}'$ be a splitting extension for $\mathfrak{m}_0$. Then $\mathfrak{m}_0$ is unramified in $\tilde{\Delta}$ over $\tilde{K}'(x)$, where $\tilde{\Delta}$ is the double field of $K$, $\tilde{K}'$. Since $\Delta\mathfrak{m} = K'$, $\mathfrak{m}$ remains a prime divisor of $\tilde{\Delta}$. Thus, $\mathfrak{m}_0$ has in $\tilde{\Delta}$ the decomposition

$$\mathfrak{m}_0 = \mathfrak{m} + \sum_{\sigma\in\underline{\sigma},\,\sigma\neq 1} \tilde{\mathfrak{m}_\sigma}$$

into prime divisors $\tilde{\mathfrak{m}_\sigma}$ with $N_{\tilde{\Delta}/\tilde{K}'}(\tilde{\mathfrak{m}_\sigma}) = 1$, where $\underline{\sigma}$ is the isomorphism system of $K\mu$ into $\tilde{K}'$. It follows that

$$(x - x\mu) = \mathfrak{m}_0 - (u_x + u_x\mu) = \mathfrak{m} + \sum_{\sigma\in\underline{\sigma},\,\sigma\neq 1} \tilde{\mathfrak{m}_\sigma} - (u_x + u_x\mu).$$

This implies that

$$-\mathfrak{n} = \sum_{\sigma\in\underline{\sigma},\,\sigma\neq 1} \tilde{\mathfrak{m}_\sigma} - (u_x + u_x\mu),$$

and hence

$$-\mathfrak{n}\mathfrak{m} = \sum_{\sigma\in\underline{\sigma},\,\sigma\neq 1} \tilde{\mathfrak{m}_\sigma}\mathfrak{m} - (u_x + u_x\mu)\mathfrak{m}.$$

It follows from the part (1) in the proof of Lemma 5.2 that

$$\tilde{\mathfrak{m}_\sigma}\mathfrak{m} = \mathfrak{D}_{\mu\sigma,\mu}.$$

Since $(u_x + u_x\mu)\mathfrak{m} = 2u_x\mu$, in order to prove that $\mathfrak{n}\mathfrak{m} + (dx)\mu$ is principal it suffices to show that

$$\mathfrak{D}_x\mu - \sum_{\sigma\in\underline{\sigma},\,\sigma\neq 1} \mathfrak{D}_{\mu\sigma,\mu}$$

is principal. But, by the approximation theorem on $K$ and [2, Theorem 6 on page 92] we have

$$\mathfrak{D}_x\mu = \sum_{\sigma\in\underline{\sigma},\,\sigma\neq 1} \mathfrak{D}_{\mu\sigma,\mu}. \quad \square$$

By Lemma 5.5 and its proof, we obtain the following useful result.

**Corollary 5.6.** *Let $\mathfrak{m}$ be a binary prime divisor of $\Delta$ with $N_{\Delta/K'}(\mathfrak{m}) = 1$. Denote by $\mu$, $\mu' = 1$ the isomorphism pair of $K$, $K'$ induced by $\mathfrak{m}$. Assume that $x$ is a separating element of $K$. Then $\langle\mathfrak{m},\mathfrak{m}\rangle_f + N_{\Delta/K}(\mathfrak{m})(dx)$ and $\langle\mathfrak{m},\mathfrak{m}\rangle_f' + (dx)\mu$ are principal.*

## 6. A residue scalar product of divisors

When $\infty$ is an infinite place of $k$, we view $K'$ as an algebraic function field of one variable over $\mathbb{C}$. Denote by $K'_\infty$ the set of all places of $K'$. If $f$ is an element of $K'$ and if $v$ is a place of $K'$, then either $v$ is a pole of $f$, in which case we say that $f$ takes the value $\infty$ at $v$, or this is not the case, and then the value $f(v)$ taken by

$f$ at $v$ (which is the residue class of $f$ modulo $v$) is a complex number. Denote by $\hat{\mathbb{C}}$ the Riemann sphere, obtained by adjunction of a point $\infty$ to $\mathbb{C}$. Consider $K'_\infty$ as a topological space whose topology is the weakest topology with respect to which the mappings $f\colon v \to f(v)$ of $K'_\infty$ into $\hat{\mathbb{C}}$ are continuous. Then $K'_\infty$ is a compact Riemann surface; see [4, Chapter VII].

Let $\mathfrak{A}$ be a divisor of $K'$. Then the extension of $\mathfrak{A}$ to $K'_\infty$ is a divisor of $K'_\infty$, and there exists a line bundle $L$ with a Hermitian metric $\|\cdot\|$ and with a meromorphic section $s$ whose divisor is the extension of $\mathfrak{A}$ to $K'_\infty$ (cf. [1, §2]). We assume that the metric $\|\cdot\|$ on $L$ satisfies

$$(\deg L)d\mu'_\infty = c_1(\|\cdot\|, L),$$

where $c_1(\|\cdot\|, L)$ is the Chern form of the metric $\|\cdot\|$ on the line bundle $L$. Define

$$\mathfrak{A}_{K'} = \mathfrak{A} + \sum_\infty \left( -\int_{K'_\infty} \log \|s\| d\mu'_\infty \right) K'_\infty,$$

where the sum is over the infinite places of $k$. Then $\mathfrak{A}_{K'}$ is an Arakelov divisor of $K'$. We call $\mathfrak{A}_{K'}$ the Arakelov divisor of $K'$ obtained from the divisor $\mathfrak{A}$. Let $\mathfrak{A}$ and $\mathfrak{b}$ be divisors of $\Delta$, relatively prime to each other. By (5.4), $\langle \mathfrak{A}, \mathfrak{b} \rangle'_f$ is a divisor of $K'$, and hence we can obtain an Arakelov divisor $\langle \mathfrak{A}, \mathfrak{b} \rangle_{K'}$ of $K'$ from the divisor $\langle \mathfrak{A}, \mathfrak{b} \rangle'_f$. By (5.4), we have $\langle \mathfrak{A}, \mathfrak{b} \rangle'_f = \langle \mathfrak{b}, \mathfrak{A} \rangle'_f$. This implies that $\langle \mathfrak{A}, \mathfrak{b} \rangle_{K'} = \langle \mathfrak{b}, \mathfrak{A} \rangle_{K'}$. If $f$ is an element of $K'$, we put $v_\infty(f) = -\int_{K'_\infty} \log |f| d\mu'_\infty$. Let $(f)_{\text{fin}}$ be the divisor of $f$ on $K'$. Then a principal Arakelov divisor is given by

$$(f)_{K'} = (f)_{\text{fin}} + \sum v_\infty(f) K'_\infty$$

where the sum is over the infinite places of $k$. It is clear that $\mathfrak{A}_{K'}$ is a principal Arakelov divisor of $K'$ if $\mathfrak{A}$ is a principal divisor of $K'$. Hence, by Theorem 4.8, $\langle \mathfrak{A}, \mathfrak{b} \rangle_{K'}$ is a principal Arakelov divisor of $K'$ if $\mathfrak{A}$ is a principal divisor of $\Delta$.

Let $x'$ be a separating element of $K'$. Denote by $dx'$ the divisor $\mathfrak{D}_{x'}/u_{x'}^2$, where $\mathfrak{D}_{x'}$ is the different of $K'$ over $k(x')$ and $u_{x'}$ is the denominator of $x'$. Then $dx'$ belongs to the class of divisors of differentials of $K'$ (cf. [5, Chapter 25]). Let $\mathfrak{d}_{K'}$ be the Arakelov divisor of $K'$ obtained from the divisor $dx'$. For every Arakelov divisor $D$ of $K'$, we define

$$\deg_{K'} D = (D \cdot \mathfrak{d}_{K'}), \tag{6.1}$$

where $(\ \cdot\ )$ is the Arakelov intersection product [1, §1]. Let $\mathfrak{A}$ and $\mathfrak{b}$ be divisors of $\Delta$, relatively prime to each other. We define

$$\langle \mathfrak{A}, \mathfrak{b} \rangle = \deg_{K'} \langle \mathfrak{A}, \mathfrak{b} \rangle_{K'}. \tag{6.2}$$

If $\mathfrak{A}$ is a divisor of $\Delta$, we denote by $\mathfrak{A}|K'$ the Arakelov divisor of $K'$ obtained from the restriction of $\mathfrak{A}$ to $K'$. If $\mathfrak{m}, \mathfrak{n}$ are two different prime divisors of $\Delta$, we define

$$\{\mathfrak{m}, \mathfrak{n}\} = N_{\Delta/K'}(\mathfrak{n}) \deg_{K'}(\mathfrak{m}|K') + N_{\Delta/K'}(\mathfrak{m}) \deg_{K'}(\mathfrak{n}|K').$$

Similarly, we define $\{\mathfrak{A}, \mathfrak{b}\}$ for all divisors $\mathfrak{A}$, $\mathfrak{b}$ of $\Delta$ by linearity.

**Definition 6.3.** *Let $\mathfrak{A}, \mathfrak{b}$ be divisors of $\Delta$ which are relatively prime to each other. Then a residue scalar product $\langle \mathfrak{A}, \mathfrak{b} \rangle_r$ of $\mathfrak{A}$ and $\mathfrak{b}$ is defined by*

$$\langle \mathfrak{A}, \mathfrak{b} \rangle_r = \{\mathfrak{A}, \mathfrak{b}\} - \langle \mathfrak{A}, \mathfrak{b} \rangle.$$

If $(f)$ is a principal divisor of $\Delta$, it follows from (6.1) and Theorem 4.8 that $\langle (f), \mathfrak{A} \rangle_r = 0$ for any divisor $\mathfrak{A}$ of $\Delta$, and hence the residue scalar product $\langle \mathfrak{A}, \mathfrak{b} \rangle_r$ is well-defined on the classes of divisors of $\Delta$ modulo principal divisors. By (5.4) and Theorem 5.3, the residue scalar product is bilinear and symmetric.

Part of Roquette's theory is to prove that the residue scalar product of a divisor of the double field with itself is nonnegative for function fields over a finite constants field by using the Riemann-Roch theorem (cf. Li [7]). Then the Riemann hypothesis for function fields over a finite constants field follows from the Schwarz inequality. Searching for the analogue for number fields of Roquette's proof of the Riemann hypothesis for function fields over a finite constants field, we were led to the sequence of numbers whose positivity is equivalent to the Riemann hypotheses [6]. We conjecture that the residue scalar product, which we constructed for function fields over a number field, of a divisor with itself is nonnegative. This nonnegativity, if true, may be related to that of the sequence of numbers found in Li [6].

## References


1. S. J. Arakelov, *Intersection theory of divisors on an arithmetic surface*, Math. USSR Izv. **8** (1974), 1167–1180.
2. E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, New York, 1967.
3. J. W. S. Cassels, *Global fields*, in "Algebraic Number Theory," Edited by J.W.S. Cassels and A. Fröhlich, Academic Press, New York, 1967, 42–75.
4. C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, Mathematical Surveys, Number VI, Amer. Math. Soc., New York, 1951.
5. H. Hasse, *Number Theory*, Springer-Verlag, New York, 1980.
6. Xian-Jin Li, *The positivity of a sequence of numbers and the Riemann hypothesis*, J. Number Theory **65** (1997), 325–333.
7. Xian-Jin Li, *A note on the Riemann-Roch theorem for function fields*, "Analytic Number Theory: Proc. Conf. in Honor of Halberstam," Edited by Berndt, Diamond and Hildebrand, Vol. 2, Birkhäuser-Verlag, 1996, 567–570.
8. P. Roquette, *Arithmetischer Beweis der Riemannschen Vermutung in Kongruenzfunktionenkörpern beliebigen Geschlechts*, J. Reine Angew. Math. **191** (1953), 199–252.
9. A. Weil, *Sur les fonctions algébriques à corps de constantes finis*, C. R. Acad. Sci. Paris **210** (1940), 592–594.



American Institute of Mathematics, 360 Portage Avenue, Palo Alto, CA 94306
*E-mail address*: `xianjin@math.Stanford.EDU`

Current address: Department of Mathematics, Brigham Young University, Provo, Utah 84602